Kemendikdasmen
Badan Standar, Kurikulum, dan Asesmen Pendidikan

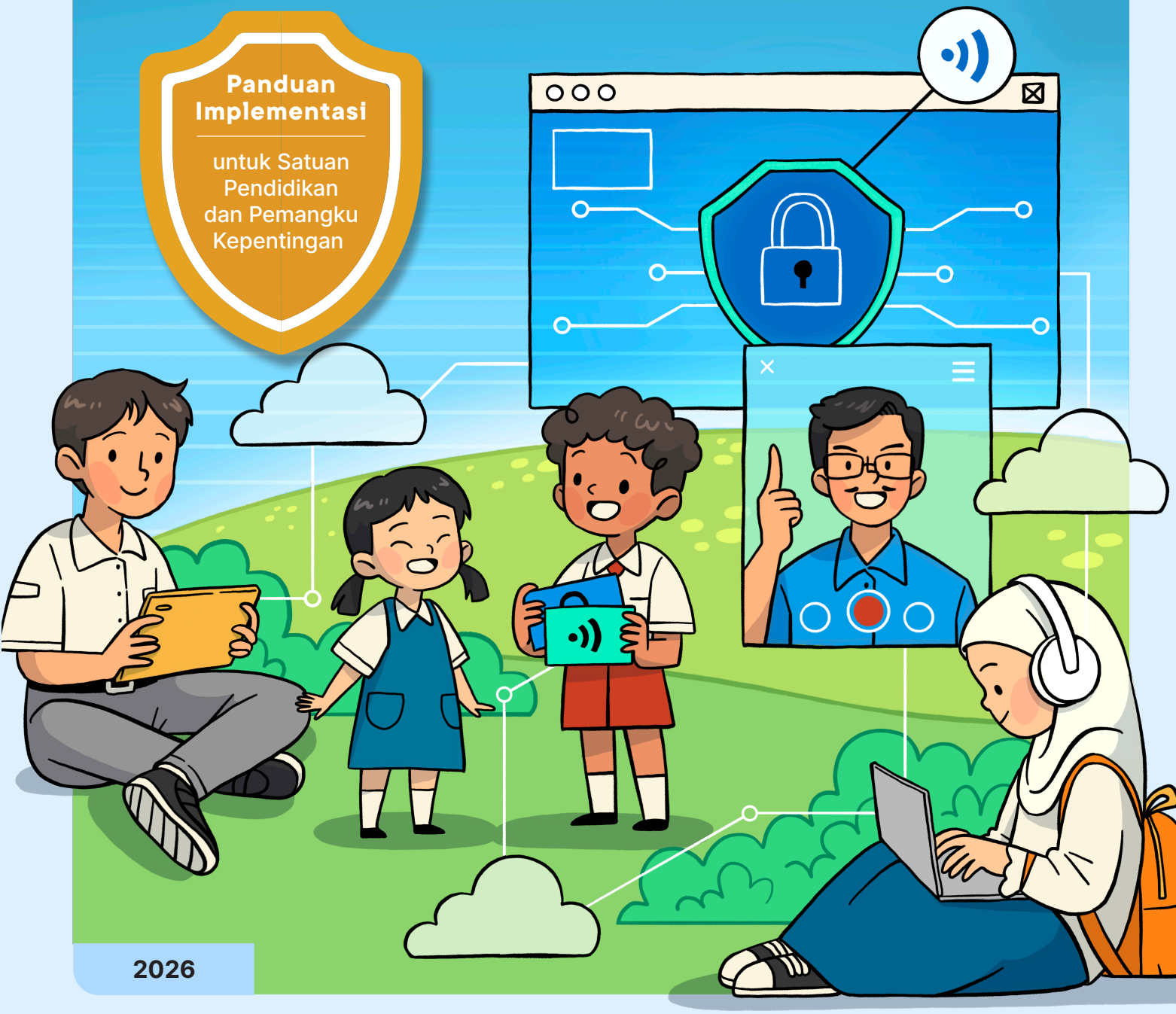
#PENDIDIKAN BERMUTU UNTUK SEMUA

KEMENDIKDASMEN RAMAH

PENDIDIKAN KEAMANAN SIBER

Panduan Implementasi

untuk Satuan Pendidikan dan Pemangku Kepentingan



2026

Panduan Implementasi Pendidikan Keamanan Siber
Untuk Satuan Pendidikan dan Pemangku Kepentingan

Pengarah
Prof. Dr. Toni Toharudin, S.Si., M.Sc., Kepala Badan Standar, Kurikulum, dan Asesmen Pendidikan

Penanggung jawab
Dr. Laksmi Dewi, M.Pd., Kepala Pusat Kurikulum dan Pembelajaran

Tim Penyusun
Mita Pramihapsari, S.S.T.MP., Badan Siber dan Sandi Negara
Listyanti Dewi Astuti, S.Pd., M.Kom., SMK Negeri 12 Malang
Fedora, B.Sc., S.Pd., M.Ed., Sekolah Citra Kasih Jakarta
Nurul Hasani, S.ST., S.H., M.Si., Badan Siber dan Sandi Negara
Rian Irawan, Badan Siber dan Sandi Negara
Septiaji Eko Nugroho, S.T, M.Sc., MAFINDO
Prof. Dr. Ir. Eko Kuswardono Budiardjo, M.Sc., Universitas Indonesia
Putu Widyarani Kusumadewi, S.T., Pusat Kurikulum dan Pembelajaran
Fijar Hafiizh, S.E., Pusat Kurikulum dan Pembelajaran

Kontributor
Mohamad Irfan, S.T.P., Pusat Kurikulum dan Pembelajaran
Harimawan Apriyanto, S.Kom., SMK Negeri 12 Malang
Suci Nurhayati Candra, M.Pd., SMK Negeri 12 Malang
Muhamad Arifin, M.Pd., SMK Telkom Malang
Sotya Renaningwibi Samsudin, S.Pd., SMK Negeri 4 Malang
Yohan Adi Setiawan, S.Kom., SMP Negeri 2 Kalitidu
Leo Andy, S.S., Sekolah Citra Berkat CitraRaya Tangerang
Muhammad Muslim Machbub Sulthony, M. Pd., SD Negeri Cibubur 10

Ilustrasi dan Tata Letak
Studio Kawa Kreatif Indonesia

Penerbit
Pusat Kurikulum dan Pembelajaran
Badan Standar, Kurikulum, dan Asesmen Pendidikan
Kementerian Pendidikan Dasar dan Menengah Republik Indonesia

2026

Kemendikdasmen
Badan Standar, Kurikulum, dan Asesmen Pendidikan

PENDIDIKAN KEAMANAN SIBER

Panduan Implementasi

untuk Satuan Pendidikan dan Pemangku Kepentingan

2026

Kata Pengantar

Puji syukur ke hadirat Allah SWT, karena atas rahmat dan karunia-Nya, Panduan Implementasi Pendidikan Keamanan Siber Untuk Satuan Pendidikan dan Pemangku Kepentingan ini dapat diselesaikan dan dihadirkan sebagai bagian dari upaya nasional untuk memperkuat literasi keamanan siber sejak usia dini. Penyusunan panduan ini berlandaskan kebijakan nasional, termasuk Rencana Aksi Nasional Keamanan Siber dan Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional, yang menegaskan pentingnya peningkatan kapasitas masyarakat dalam menghadapi risiko dan ancaman di ruang siber.

Seiring meningkatnya penggunaan teknologi digital dalam proses belajar, bermain, dan berinteraksi, murid semakin rentan terhadap berbagai risiko di ruang siber. Beragam insiden seperti penyalahgunaan akses, penipuan daring, perundungan daring, hingga paparan konten berbahaya menunjukkan perlunya pembekalan kompetensi keamanan siber yang terstruktur. Kondisi tersebut menjadi dasar perlunya panduan ini sebagai acuan yang adaptif bagi satuan pendidikan untuk mengembangkan literasi keamanan siber sesuai kebutuhan dan konteks masing-masing.

Pendidikan keamanan siber bukan semata-mata pengetahuan teknis, tetapi merupakan bagian penting dari kecakapan hidup abad ke-21. Melalui panduan ini, murid diharapkan memiliki pengetahuan yang benar, sikap yang bijak, dan perilaku yang aman dalam beraktivitas di ruang siber. Dengan menumbuhkan kebiasaan positif dan budaya sadar risiko, diharapkan tercipta karakter digital yang berlandaskan nilai kejujuran, tanggung jawab, dan penghormatan terhadap sesama.

Kami menyadari bahwa buku ini masih memiliki keterbatasan baik dari segi isi maupun penyusunan. Oleh karena itu, kami membuka diri terhadap masukan, koreksi, dan saran dari satuan pendidikan, pendidik, serta pemangku kepentingan terkait guna penyempurnaan panduan ini pada edisi berikutnya.

Pada akhirnya, kami menyampaikan terima kasih kepada seluruh tim penyusun, para ahli, serta pemangku kepentingan yang telah berkontribusi dalam penyusunan panduan ini. Semoga panduan ini dapat dimanfaatkan oleh satuan pendidikan, pendidik, orang tua, dan murid untuk membangun lingkungan belajar yang aman, sehat, dan tangguh di ruang siber, guna mendukung terwujudnya generasi emas Indonesia 2045.

Kepala Badan Kurikulum, dan Asesmen Pendidikan

Prof. Dr. Toni Toharudin, S.Si., M.Sc

Pengantar Panduan

Mengapa?

Keamanan Siber adalah upaya adaptif dan inovatif untuk melindungi seluruh lapisan ruang siber, termasuk aset informasi yang ada di dalamnya, dari ancaman dan serangan siber, baik yang bersifat teknis maupun sosial. Indonesia termasuk dalam negara dengan risiko tinggi terhadap ancaman siber seiring dengan percepatan transformasi digital dan penggunaan teknologi informasi yang meluas. Kerentanan tersebut semakin bertambah karena pemahaman umum tentang keamanan siber masih terbatas.

Data statistik menunjukkan bahwa anak-anak Indonesia mengakses internet sejak usia dini, tetapi sering kali belum memiliki kemampuan yang memadai untuk mengenali risiko, bersikap kritis, atau mengambil keputusan aman di ruang siber. Karenanya, mereka berhak memperoleh informasi, literasi, dan perlindungan sehingga dapat berpartisipasi secara produktif dalam ruang siber yang aman.

Untuk apa?

Pendidikan keamanan siber bertujuan untuk membekali murid dengan pengetahuan keamanan siber, pemahaman bersikap bijak di ruang siber serta kemampuan dalam menerapkan perilaku yang aman di ruang siber. Pendidikan keamanan siber merupakan salah elemen yang mendukung kompetensi abad 21 dan selaras dengan tujuan pendidikan nasional, yaitu membentuk warga negara yang cerdas, bertanggung jawab, dan berkarakter.

Selain melindungi diri dari ancaman siber, pendidikan keamanan siber juga memberikan manfaat tidak langsung bagi perkembangan anak, seperti peningkatan kemampuan analitis, penguatan etika digital, serta kemampuan menavigasi informasi dengan bijak.

Untuk siapa?

Panduan ini ditujukan bagi seluruh penyelenggara ekosistem pendidikan, termasuk pimpinan satuan pendidikan, pendidik, tenaga kependidikan, murid, dan orang tua. Selain itu, panduan ini relevan bagi pemangku kepentingan lain seperti pemerintah daerah, lembaga pelatihan, organisasi masyarakat sipil, komunitas digital, dan pelaku industri teknologi yang berperan dalam memperkuat budaya keamanan siber di lingkungan pendidikan.

Kapan, di mana, dan bagaimana?

Panduan ini memberikan prinsip, strategi, dan langkah-langkah praktis bagi satuan pendidikan untuk menerapkan pendidikan keamanan siber secara efektif di berbagai konteks pembelajaran dalam bentuk intrakurikuler, kokurikuler, ekstrakurikuler, maupun budaya sekolah. Panduan ini juga dilengkapi contoh kegiatan, materi pembelajaran, referensi sumber belajar, serta jejaring kemitraan yang dapat dimanfaatkan agar implementasi pendidikan keamanan siber berjalan sesuai dengan prinsip pembelajaran yang aman, inklusif, dan berkualitas.

Cara Menggunakan Panduan Ini

Dokumen ini disusun untuk membantu kepala sekolah, pendidik, dan pihak terkait dalam menerapkan pendidikan keamanan siber di lingkungan satuan pendidikan. Untuk memudahkan penggunaannya, panduan ini bersifat modular, sehingga setiap pengguna dapat langsung menuju bab atau subbab yang sesuai dengan kebutuhan, tanpa harus membaca seluruh bagian secara berurutan.

Panduan ini juga bersifat adaptif. Artinya, satuan pendidikan dipersilakan menyesuaikan materi, strategi, dan contoh penerapan dengan konteks lokal, seperti karakteristik murid, kesiapan guru, ketersediaan gawai, serta akses internet di sekolah atau rumah.

Berikut panduan penggunaan secara umum:

1. Identifikasi peran pengguna (kepala sekolah, pendidik, atau mitra eksternal).
2. Pilih bab yang relevan berdasarkan peran dan kebutuhan.
3. Sesuaikan penerapan dengan kondisi satuan pendidikan.
4. Jika diperlukan, gunakan contoh situasi pada setiap bab sebagai inspirasi pengembangan kegiatan.

Isi Setiap Bab	
Bab 1	Pengantar konsep ruang siber, manfaat, risiko, dan cara melindungi diri.
Bab 2	Esensi, tujuan, prinsip, dan kerangka kompetensi pendidikan keamanan siber per jenjang pendidikan.
Bab 3	Peran kepemimpinan sekolah dalam memastikan budaya dan kebijakan keamanan siber berjalan efektif.

Bab 4	Penerapan pendidikan keamanan siber dalam kegiatan intrakurikuler, kokurikuler, dan ekstrakurikuler, serta contoh praktik baik.
Bab 5	Kolaborasi dengan pihak di luar satuan pendidikan dan contoh bentuk peran yang dapat dilakukan untuk memperkuat ekosistem keamanan siber.
Lampiran	Dokumen pendukung panduan, diantaranya Peta Kompetensi Pendidikan Keamanan Siber untuk tiap jenjang beserta rekomendasi aktivitas dalam implementasinya, contoh integrasi Pendidikan Keamanan Siber ke dalam intrakurikuler dan kokurikuler, serta contoh MoU kerja sama antara sekolah dan lembaga dalam rangka pengembangan Pendidikan Keamanan Siber.

Tahukah Anda

Bagian ini menyajikan fakta menarik, fenomena, atau gambaran awal terkait keamanan siber untuk membangun rasa ingin tahu dan pemahaman konteks.

Praktik Baik

Bagian ini menampilkan contoh pengalaman, inisiatif, atau pembelajaran dari sekolah-sekolah yang telah menerapkan pendidikan keamanan siber.

Fakta Data

Bagian ini memuat data, statistik, atau temuan berbasis bukti yang relevan untuk memperkuat pemahaman dan menunjukkan kondisi nyata keamanan siber.

Informasi Penting

Bagian ini menyoroti hal-hal krusial yang perlu diperhatikan dalam penyelenggaraan pendidikan keamanan siber di sekolah.

Kata Kunci

Bagian ini berisi istilah-istilah penting yang perlu dipahami dalam pembelajaran keamanan siber.

Daftar Isi

Daftar Istilah

Akun Digital	Identitas pengguna di platform digital yang dilindungi dengan nama pengguna dan kata sandi.
Ancaman Siber	Segala bentuk potensi bahaya atau tindakan yang dapat mengganggu, merusak, atau mengambil alih perangkat, data, atau aktivitas digital seseorang.
Aplikasi	Perangkat lunak yang digunakan untuk menjalankan fungsi tertentu di perangkat digital.
Autentikasi Ganda/ Dua Faktor (*Two-Factor Authentication*)	Mekanisme keamanan tambahan untuk memastikan keaslian pengguna akun digital.
Budaya Keamanan Siber	Kebiasaan, nilai, dan sikap yang membentuk perilaku aman dan bertanggung jawab di dunia digital.
Computer Security Incident Response Team **(CSIRT)**	Tim Tanggap Insiden Siber (TTIS) yang bertanggung jawab menangani insiden siber sesuai ruang lingkupnya.
Data Pribadi	Informasi tentang seseorang yang dapat mengidentifikasi individu tersebut, baik langsung maupun tidak langsung.
Etika Digital	Norma dan nilai moral dalam berinteraksi dan berperilaku di dunia maya.
Ekstrakurikuler	Kegiatan pendidikan di luar jam pelajaran kurikulum standar yang dilakukan di sekolah atau luar sekolah, bertujuan untuk mengembangkan bakat, minat, kepribadian, kemampuan, dan potensi peserta didik secara optimal

Gawai (*Gadget*)	Alat elektronik portabel yang digunakan untuk berkomunikasi, mengakses internet, dan menjalankan aplikasi digital.
Hoaks	Informasi palsu atau menyesatkan yang disebarkan secara sengaja atau tidak di ruang digital.
Identitas Daring	Representasi diri seseorang di dunia maya melalui akun, profil, dan aktivitas digital.
Jejak Digital	Rekam jejak aktivitas pengguna di internet, baik yang disengaja maupun tidak.
Jaringan Internet	Sistem komunikasi global yang menghubungkan perangkat dan pengguna di seluruh dunia.
Kata Sandi (*Password*)	Kunci rahasia untuk melindungi akses terhadap akun digital.
Keamanan Siber (*Cybersecurity*)	Upaya adaptif dan inovatif untuk melindungi seluruh lapisan ruang siber termasuk aset informasi yang ada di dalamnya, dari ancaman dan serangan siber, baik bersifat teknis maupun sosial.
Kejahatan Siber	Segala bentuk tindakan melanggar hukum yang dilakukan dengan menggunakan komputer, perangkat digital, jaringan, atau internet, yang bertujuan merugikan individu, kelompok, atau organisasi.
Insiden Siber	Suatu peristiwa dan rangkaian kejadian yang mengganggu kerahasiaan, integritas, atau ketersediaan data dan layanan digital. Misalnya akun anak diretas, data kelas bocor, atau perangkat terkena malware.
Intrakurikuler	Kegiatan pembelajaran untuk mencapai tujuan belajar sesuai jadwal dan beban belajar pada struktur kurikulum.

Kokurikuler	Kegiatan pembelajaran yang dilaksanakan untuk penguatan, pendalaman, dan/atau pengayaan mata pelajaran yang telah dipelajari dalam kegiatan intrakurikuler di kelas, sebagai upaya untuk mengoptimalkan penguatan pendidikan karakter pada murid.
Literasi Digital	Kemampuan memahami, menggunakan, dan mengevaluasi informasi digital secara kritis dan etis.
***Malware* (*Malicious Software*)**	Program berbahaya seperti virus, trojan, atau ransomware yang dapat merusak perangkat.
Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)	Regulasi yang mengatur segala bentuk informasi, transaksi elektronik, dan sanksi pidana terhadap penyalahgunaan teknologi digital atau internet.
Undang-Undang Pelindungan Data Pribadi (UU PDP)	Regulasi menjamin keamanan dan hak privasi setiap orang atas data pribadinya, baik dalam sistem elektronik maupun nonelektronik, serta menetapkan sanksi bagi penyalahgunaan data tersebut.
Penipuan Daring (*Online Scam*)	Upaya menipu pengguna untuk mendapatkan uang atau data pribadi secara ilegal.
Perangkat Digital	Semua alat elektronik yang memproses, menyimpan, atau menampilkan informasi dalam bentuk digital.
Perundungan Daring (*Cyberbullying*)	Tindakan agresif atau intimidatif yang dilakukan melalui platform digital.
Penyelenggara Sistem Elektronik (PSE)	Pihak yang menyediakan, mengelola, dan/atau mengoperasikan layanan berbasis elektronik.
Phishing	Upaya penipuan untuk mencuri informasi dengan cara menyamar sebagai pihak terpercaya, biasanya melalui pesan, email, atau tautan palsu.

Privasi	Hak setiap individu untuk mengendalikan informasi tentang dirinya, termasuk bagaimana data tersebut dikumpulkan, digunakan, disimpan, dan dibagikan oleh pihak lain. Dalam konteks digital, privasi mencakup pengaturan siapa yang dapat melihat aktivitas, identitas, dan data pribadi seseorang di internet.
RAN Keamanan Siber Nasional	Rencana aksi nasional untuk meningkatkan keamanan siber Indonesia.
Reputasi Daring	Citra atau penilaian seseorang di dunia maya yang terbentuk dari jejak digital, perilaku, dan interaksi online.
Risiko Siber	Kemungkinan terjadinya ancaman siber *ditambah* besarnya dampak yang ditimbulkan terhadap individu atau lingkungan digital.
Ruang Siber (*Cyberspace*)	Lingkungan virtual tempat berlangsungnya aktivitas digital manusia melalui internet dan perangkat elektronik.

BAB
1

Mengenal Ruang Siber bagi Anak

BAB 1

Mengenal Ruang Siber bagi Anak

A Apa itu Ruang Siber?

Beberapa dekade lalu, dunia anak-anak Indonesia dibatasi oleh ruang yang jelas terlihat, seperti rumah, sekolah, taman bermain, atau lapangan di dekat rumah. Orang tua bisa dengan mudah mengawasi dengan siapa anak bermain, apa yang dilakukan, dan kapan mereka pulang. Kini, ruang hidup anak-anak mengalami perubahan besar. Seiring dengan hadirnya gawai, komputer, dan konektivitas internet, anak-anak tumbuh di sebuah dunia baru yang tidak kasat mata tetapi terasa begitu nyata: ruang siber. Ruang baru ini membuka kesempatan belajar, berkreasi, dan berinteraksi yang jauh lebih luas dari pada sebelumnya.

Secara konsep, ruang siber (*cyberspace*) dapat dipahami sebagai ruang abstrak yang terbentuk dari interaksi jaringan komputer, perangkat digital, dan koneksi internet. Di dalamnya berlangsung komunikasi, transaksi, produksi informasi, bahkan pembentukan identitas diri. Shapiro (1999) menyebut ruang siber sebagai "lingkungan sosial virtual" yang beroperasi 24 jam, tanpa batas geografis dan sering kali tanpa batas otoritas. Dengan membayangkan ruang siber sebagai taman bermain digital raksasa, kita dapat memahami bahwa banyak hal baik yang bisa didapatkan selama ada aturan, pendampingan dan literasi keamanan yang memadai.

Bagi anak-anak, ruang siber ibarat kota maya yang penuh peluang. Ada "sekolah" berupa platform belajar daring, "perpustakaan" melalui mesin pencari, "taman bermain" lewat gim daring, "pasar" melalui *e-commerce*, dan "bioskop" lewat layanan *streaming*. Dengan pemahaman dan kebiasaan aman yang tepat, ruang ini dapat menjadi tempat yang memperkaya pengalaman belajar dan tumbuh kembang. Namun, seperti halnya kota di dunia nyata, ruang siber tetap memerlukan kewaspadaan agar anak terhindar dari pengalaman yang tidak menyenangkan. Oleh karena itu, pendekatan yang paling penting adalah membekali anak dengan **pendidikan keamanan siber**. Sehingga anak-anak dapat menikmati manfaat ruang siber secara aman, bertanggung jawab, dan percaya diri.

Tahukah Anda

Dulu banyak orang memahami internet hanya sebatas halaman web yang dibuka lewat *browser,* padahal seiring perkembangan teknologi kita belajar bahwa **internet** adalah jaringan global yang menghubungkan miliaran perangkat untuk bertukar data, sementara **World Wide Web (WWW)** hanyalah salah satu layanan di dalamnya yang berisi halaman-halaman yang saling terhubung. Ketika aplikasi pesan, gim daring, video pendek, dan platform belajar muncul, aktivitas digital manusia meluas menjadi apa yang kini dikenal sebagai **ruang siber**, yaitu tempat berbagai layanan, interaksi, dan data saling terhubung secara digital. Perkembangannya bahkan semakin jauh dengan hadirnya **Internet of Things (IoT)**, yaitu perangkat fisik seperti jam tangan pintar, CCTV, smart TV, dan mesin absen sekolah yang dapat terhubung ke internet dan saling bertukar data.

B Siapa yang ada di Ruang Siber?

Sama halnya dengan dunia nyata, ruang siber dapat diibaratkan sebagai sebuah kota besar yang dinamis, tempat anak-anak menjadi bagian dari populasi global yang sangat beragam. Di kota virtual ini, anak-anak tidak hanya bertemu dengan teman sebaya dari sekolah, tetapi juga berkesempatan berjumpa dengan orang-orang dari berbagai latar belakang, profesi, dan minat dari seluruh dunia. Interaksi tanpa batas geografis ini memperkaya pengalaman sosial dan membuka akses terhadap beragam perspektif, sekaligus menuntut kewaspadaan yang lebih tinggi.

Survei UNICEF (2023) mencatat bahwa 4 dari 10 anak di Asia Tenggara pernah menerima pesan dari orang asing secara daring. Temuan ChildFund (2022) juga menegaskan bahwa anak-anak semakin sering berinteraksi dengan orang yang tidak mereka kenal di internet baik melalui gim, media sosial, maupun aplikasi pesan. Sebagian besar interaksi ini bersifat netral atau bahkan positif, seperti ajakan bermain gim atau berbagi minat. Namun sebagian kecil dapat berubah menjadi upaya manipulatif, misalnya meminta informasi pribadi, mengajak pindah ke platform lain, atau menawarkan hadiah palsu. Informasi seperti ini penting untuk dipahami agar orang tua dan anak dapat mengenali tanda-tanda interaksi yang tidak sehat sejak awal.

Di sisi lain, ruang siber juga dipenuhi banyak figur positif yang memberi peluang belajar. Ada guru dan dosen yang membagikan materi ajar, influencer edukasi yang menampilkan eksperimen sains sederhana, konten kreator literasi, dokter yang berbagi edukasi kesehatan, hingga penggiat literasi yang mengajarkan keamanan siber. Interaksi ini memberi kesempatan bagi anak untuk menemukan inspirasi baru dan memperluas wawasan.

Ruang siber juga merupakan arena profesional di mana banyak orang bekerja dengan serius menjaga keamanan, merancang sistem, dan melindungi data dari ancaman siber. Di ruang ini terdapat berbagai profesi seperti auditor keamanan, ahli forensik komputer, pengembang perangkat lunak keamanan, hingga *incident responder* yang semuanya berperan dalam menjaga ruang siber tetap aman dan terpercaya. Pemahaman yang seimbang seperti ini membantu guru menyampaikan bahwa profesi di dunia digital sangat luas, tidak selalu identik dengan risiko, dan bisa menjadi inspirasi karier masa depan.

Namun, perlu dipahami bahwa salah satu karakter khas ruang siber adalah anonimitas. Yaitu, kemudahan seseorang untuk menyembunyikan atau memodifikasi identitasnya. Di dunia fisik, anak dapat melihat wajah dan mendengar suara langsung, tetapi di ruang siber seseorang dapat menggunakan nama samaran, foto profil palsu, atau persona tertentu. Karena itulah, interaksi di ruang siber memerlukan kebiasaan aman: berhati-hati membagikan informasi pribadi, mengenali tanda-tanda manipulasi, serta berdiskusi dengan orang tua atau pendamping ketika merasa tidak nyaman.

C Apa yang Dilakukan Anak Indonesia di Ruang Siber?

Anak Indonesia terhubung dengan ruang siber sejak usia sangat dini. Lebih dari sepertiga anak PAUD sudah menggunakan gawai untuk menonton kartun, bermain gim ringan, atau mencoba aplikasi belajar (BPS 2024). Seiring bertambah usia, aktivitas digital semakin luas: 93% remaja aktif di media sosial dan 1 dari 3 mulai bereksperimen dengan kecerdasan artifisial untuk membuat konten (UNICEF 2025). Internet juga berfungsi sebagai sarana belajar, membantu anak mengerjakan tugas dan mencari materi tambahan (UNICEF 2023).

Secara global, penggunaan internet oleh anak dan remaja tumbuh pesat dan semakin produktif (EU Kids Online 2020; ITU 2022). Namun, peluang ini disertai risiko: meningkatnya perundungan daring, paparan konten tidak layak, eksploitasi, serta lingkungan risiko campuran antara dunia nyata dan daring (ChildFund 2022–2025). Selain itu, adanya fenomena seperti *nomophobia* menunjukkan semakin kuatnya keterikatan anak pada perangkat digital.

Kata Kunci

Nomophobia (singkatan dari *no-mobile-phone phobia*) adalah kondisi **kecemasan berlebih** yang muncul ketika seseorang **tidak memegang ponsel**, kehilangan akses internet, baterai habis, atau tidak dapat memeriksa notifikasi. Pada anak dan remaja, nomophobia sering terlihat dalam bentuk:

- **Gelisah** saat ponsel jauh dari jangkauan
- **Takut ketinggalan informasi** (FOMO)
- **Keinginan terus-menerus memeriksa notifikasi**
- **Sulit fokus** pada kegiatan tanpa gawai
- **Rasa aman bergantung pada koneksi dan perangkat**

Istilah ini tidak selalu berarti "fobia klinis", tetapi menggambarkan **ketergantungan emosional dan perilaku** terhadap perangkat digital yang semakin umum terjadi di kalangan anak dan remaja.

Dalam perspektif Bronfenbrenner, ruang siber kini menjadi bagian dari *microsystem* anak. Yaitu, ruang tempat mereka berinteraksi langsung. Karena itu, pendidikan keamanan siber dan pendampingan orang tua menjadi penting sejak usia dini.

"Aktivitas Anak Indonesia di Ruang Siber: Dari Konsumen Hingga Kreator"

Menikmati hiburan	Bermedia sosial	Belajar	Berkreasi
			
Menonton Kartun, bermain game,	Berinteraksi di media sosial	Mengerjakan tugas sekolah, menonton video pembelajaran.	membuat video, gambar, musik, eksperimen AI generatif, monetisasi konten.
> ⅓ anak PAUD sudah memakai gawai (BPS 2024)	93% anak pakai medsos (UNICEF 2025).	Anak aktif mencari materi tambahan (UNICEF 2023).	1 dari 3 anak mencoba AI generatif (UNICEF 2025).

Tahukah Anda

Penggunaan internet oleh anak Indonesia terus meningkat pada 2024–2025. Kementerian Komunikasi dan Digital (Komdigi) melaporkan bahwa **48% pengguna internet nasional merupakan anak di bawah usia 18 tahun**, menjadikan kelompok ini sebagai pengguna terbesar di ruang digital (Komdigi, 2025). Laporan yang sama juga menegaskan bahwa sebagian besar anak mengakses internet lebih dari lima jam per hari melalui ponsel.

Data Badan Pusat Statistik (BPS) melalui *Profil Anak Indonesia 2024* menunjukkan bahwa **39,71% anak usia dini telah menggunakan ponsel**, dan **35,57% diantaranya sudah mengakses internet** (BPS, 2024). Bahkan, pada kelompok usia < 1 tahun, tercatat **5,88% bayi sudah menggunakan ponsel**, sedangkan **4,33%** memiliki paparan internet (Diskominfo Kaltim, 2025). Temuan ini menegaskan bahwa penetrasi digital dimulai jauh sebelum anak memahami risiko maupun tata kelola penggunaan perangkat.

D Peluang Positif dari Aktivitas Anak di Ruang Siber

Ruang siber yang sehat membuka akses luas bagi anak-anak Indonesia untuk belajar, berekspresi, dan berinteraksi. Dengan pendampingan yang memadai, ruang siber dapat menjadi lingkungan yang memperkaya pengalaman pendidikan, sosial, dan pengembangan diri. Internet memungkinkan anak mengakses sumber belajar global, mengembangkan kreativitas, dan memperoleh keterampilan masa depan yang relevan dengan perkembangan teknologi.

Bagi anak usia prasekolah, perangkat digital dapat menjadi pintu pertama untuk mengenal huruf, angka, warna, atau lagu. Aplikasi interaktif membantu pembelajaran melalui kombinasi visual, audio, dan simulasi sederhana. Studi dari *American Academy of Pediatrics* (AAP, 2022) menyebutkan bahwa penggunaan teknologi dalam durasi terbatas dan dengan pendampingan dapat mendukung kemampuan kognitif dasar seperti pengenalan bentuk, bahasa, dan koordinasi motorik halus. Di Indonesia, Badan Pusat Statistik (2024) mencatat bahwa lebih dari sepertiga anak usia dini telah berinteraksi dengan gawai, sebagian besar untuk menonton video edukatif atau menyanyi bersama.

Dalam konteks pendidikan formal, pemanfaatan ruang siber memberikan nilai tambah bagi proses pembelajaran di sekolah. Guru menggunakan platform digital untuk penguatan literasi dan numerasi, sedangkan siswa dapat mengakses materi tambahan di luar ruang kelas. Di tingkat remaja, internet membuka kesempatan untuk berkreasi melalui pembuatan konten visual, audio, dan multimedia. Aktivitas ini tidak hanya mengembangkan kreativitas, tetapi juga kemampuan komunikasi dan kolaborasi.

Akses Pengetahuan Global

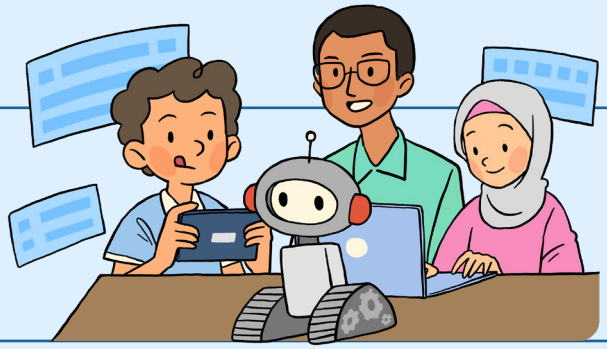
70% anak gunakan internet untuk belajar (UNICEF, 2023).

Kreativitas Digital

4 dari 10 remaja buat/bagikan konten digital (Kominfo, 2024).

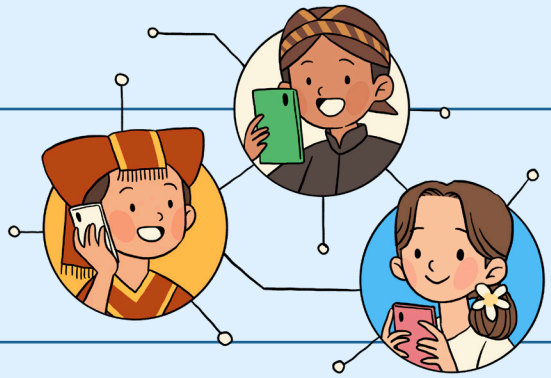
Keterampilan Masa Depan

Banyak pelajar ikut pelatihan coding & keamanan siber (Kominfo, 2024).



Jejaring Sosial Positif

86,5% anak gunakan internet untuk berteman (UNICEF, 2023).



Peluang Ekonomi Dini

Remaja mulai berjualan atau berkreasi digital bernilai ekonomi.

Potret-potret di atas menunjukkan bahwa dunia digital sebenarnya dapat menjadi mitra penting dalam perjalanan tumbuh kembang anak. Ruang siber dapat berfungsi sebagai "ruang kelas tambahan," "taman bermain kreatif," dan "laboratorium masa depan" yang mendorong perkembangan kognitif, sosial, emosional, serta keterampilan teknologi.

Namun, peluang tersebut hanya dapat diwujudkan apabila anak berada di lingkungan digital yang aman, dibekali dengan pendidikan keamanan siber yang memadai dan keterlibatan aktif orang dewasa. Di sisi lain, setiap peluang yang ditawarkan ruang siber juga berdampingan dengan potensi risiko. Pertanyaan yang muncul kemudian adalah: **jika manfaatnya begitu besar, ancaman apa saja yang justru mengintai anak-anak Indonesia di ruang siber?**

E Ancaman Siber: Seberapa Nyata?

Sama halnya dengan ruang publik di dunia nyata, di ruang siber terdapat dua sisi yang berjalan berdampingan: jalur terang yang membuka peluang belajar, berkreasi, dan bersosialisasi, serta lorong gelap yang menyimpan berbagai risiko. EU Kids Online (Livingstone dkk., 2007–2020) menegaskan bahwa setiap peluang digital selalu diiringi oleh potensi ancaman, terutama ketika anak memasuki ruang siber tanpa pendampingan dan literasi yang memadai.

Bagi anak-anak, manfaat ruang siber sering terlihat jelas dan mudah dinikmati, sementara risikonya kerap terselubung. Ancaman tidak selalu muncul dalam bentuk ekstrim seperti pemerasan seksual atau peretasan. Sebagian besar justru hadir dalam bentuk keseharian, misalnya komentar kasar, hoaks, tautan *phishing*, pesan manipulatif, atau iklan yang dirancang untuk memprofilkan anak sebagai konsumen. Tantangan lain adalah ketika anak mulai berperan bukan hanya sebagai korban, tetapi juga pelaku, misalnya ikut menyebarkan hoaks, melakukan perundungan, atau mencoba peretasan ringan tanpa memahami konsekuensi etik dan hukumnya.

Untuk memahami kompleksitas risiko digital yang dihadapi anak, **OECD dalam berbagai kajiannya mengadopsi tipologi risiko digital anak yang dikenal sebagai kerangka 4C (*Content, Contact, Conduct*, dan *Contract*)**, sebagaimana dikembangkan dalam literatur riset oleh Livingstone dan Stoilova.

Tipologi ini mengelompokkan risiko ke dalam **Risiko Konten, Risiko Kontak, Risiko Perilaku,** dan **Risiko Komersial**. Di luar tipologi 4C tersebut, perkembangan teknologi digital mutakhir, termasuk algoritma berbasis AI, datafication, dan sistem pengawasan digital memunculkan **risiko sistemik** yang semakin relevan dalam konteks perlindungan anak dan tata kelola ruang digital.

Untuk memahami kompleksitas tersebut, *OECD Digital Risks Framework* mengidentifikasi lima kelompok risiko utama yang relevan untuk anak:

Kerangka ini membantu melihat bahwa ancaman yang dihadapi anak tidak hanya teknis (seperti virus atau *malware*), tetapi juga sosial, psikologis, ekonomi, dan struktural. Risiko-risiko tersebut juga berbeda tingkat relevansinya antar jenjang usia. Karena itu, guru dan orang tua perlu memahami ancaman sesuai fase perkembangan anak.

Tabel pada Lampiran 6 merangkum jenis-jenis ancaman ruang siber yang umum menargetkan anak, beserta modus dan dampaknya. Banyaknya ancaman menunjukkan bahwa anak-anak memiliki risiko yang bersifat multidimensi karena tidak hanya terkait kriminalitas, tetapi juga aspek psikologis, sosial, ekonomi, dan teknis. Karena itu, pelindungan anak tidak hanya berbicara soal memblokir situs berbahaya, tetapi mencakup literasi keamanan, pendampingan orang dewasa, serta keterampilan keamanan siber yang membuat anak mampu mengidentifikasi risiko sendiri.

Dengan pendekatan yang komprehensif, ruang siber dapat menjadi lingkungan belajar, bermain, dan berkreasi yang aman bagi kesehatan fisik dan mental. Karena itu, penting menjaga keseimbangan dalam penggunaan teknologi. Anak-anak perlu dilindungi agar tidak menjadi korban kejahatan siber, diarahkan agar tidak terjerumus menjadi pelaku kejahatan, sekaligus didukung untuk mengembangkan keterampilan keamanan siber yang bermanfaat. Dengan begitu, ruang siber dapat menjadi ruang belajar dan berkreasi yang aman.

F Faktor-faktor yang Meningkatkan Kerentanan Anak di Ruang Siber

Ruang siber menyediakan peluang yang sangat besar, namun anak-anak menghadapi tingkat kerentanan yang tinggi terhadap risiko yang menyertainya. Kerentanan ini muncul dari interaksi berbagai faktor yang kompleks dan berlapis yang timbul oleh serangkaian faktor yang bersifat kolektif. Faktor-faktor tersebut berinteraksi dan membentuk jaringan kerentanan yang dapat dikelompokkan menjadi empat pilar utama: **Faktor Individu, Faktor Lingkungan Sosial, Faktor Pengasuhan & Keluarga,** dan **Faktor Sistem & Ekosistem Digital.**

1. Faktor Individu

Anak masih dalam tahap perkembangan sehingga belum sepenuhnya mampu mengelola risiko digital.

- Literasi digital masih terbatas
- Kontrol diri belum matang
- Lebih sensitif secara emosional & butuh pengakuan

Catatan Penting:
Anak belum siap secara kognitif dan emosional untuk menghadapi risiko di internet.

SUMBER: UNICEF (2017); WHO (2020)

2. Faktor Sosial

Lingkungan sosial memengaruhi perilaku anak di dunia digital secara signifikan.

- Tekanan dari teman sebaya
- Keinginan untuk diterima atau populer
- Budaya viral dan pencarian "likes"

Catatan Penting:
Anak terdorong mengikuti norma kelompok meskipun berisiko tinggi.

SUMBER: EU Kids Online (2020); Livingstone & Helsper (2007)

3. Faktor Keluarga

Peran orang tua sangat menentukan tingkat keamanan anak saat berselancar online.

- Kurangnya pendampingan internet
- Aturan penggunaan yang tidak jelas
- Minim komunikasi risiko digital

Catatan Penting:
Pengawasan dan edukasi dari keluarga seringkali belum optimal.

SUMBER: OECD (2021); UNICEF (2017)

4. Faktor Sistem Digital

Lingkungan digital memiliki karakteristik teknis yang meningkatkan paparan risiko.

- Algoritma konten ekstrem/sensasional
- Fitur platform yang dapat disalahgunakan
- Ketimpangan akses dan literasi

Catatan Penting:
Sistem digital belum sepenuhnya dirancang aman bagi anak (Safety by Design).

SUMBER: OECD (2021); UNICEF (2017)

Kerentanan anak di ruang siber yang kompleks menunjukkan bahwa **pelindungan terbaik bukanlah pada perangkat**, **melainkan pada kapasitas kritis anak**. sehingga, anak-anak perlu dibekali dengan kesadaran kritis sejak dini dan kemampuan untuk mengelola risiko di ruang siber. Pendidikan adalah investasi terbesar kita untuk memastikan ruang siber sepenuhnya menjadi peluang, bukan ancaman.

G Apa yang Bisa Kita Lakukan untuk Melindungi Diri?

Melindungi diri di ruang siber bukan hanya soal menjauh dari bahaya, melainkan tentang menyiapkan bekal agar anak mampu bersikap bijak, tangguh, dan bertanggung jawab dalam setiap langkah digitalnya. Bekal itu terwujud dalam kemampuan mengenali risiko, menjaga data, beretika, menguasai keterampilan teknis, dan memahami konsekuensi hukum yang menyertai.

Melindungi diri berarti menumbuhkan kesadaran akan ancaman yang mungkin hadir kapan saja. Dengan kesadaran, anak belajar membedakan mana yang aman dan mana yang patut dicurigai, serta memahami bahwa kehati-hatian adalah perisai pertama dalam berinteraksi di ruang siber.

Melindungi diri berarti menjaga data pribadi dan menyadari jejak digital yang ditinggalkan. Anak perlu memahami bahwa informasi pribadi adalah sesuatu yang berharga, dan setiap jejak yang ditorehkan dapat berdampak pada dirinya di masa kini maupun mendatang.

Melindungi diri berarti berpegang pada etika dan perilaku yang bertanggung jawab. Anak harus menyadari bahwa ruang siber adalah ruang sosial, di mana sikap saling menghargai, menolak perundungan, serta tidak menyebarkan informasi palsu menjadi bagian dari pelindungan terhadap diri sendiri sekaligus terhadap orang lain.

Melindungi diri berarti memiliki keterampilan teknis yang memadai. Mulai dari membuat kata sandi yang kuat, menggunakan autentikasi berlapis, hingga mampu mengenali ancaman teknis pada perangkat. Dengan keterampilan ini, anak tidak hanya memahami risiko, tetapi juga memiliki cara nyata untuk menghindarinya.

Melindungi diri berarti memahami bahwa setiap tindakan di ruang siber memiliki konsekuensi hukum. Anak belajar bahwa melanggar privasi, melanggar hak cipta, atau melakukan perundungan daring bukan hanya keliru secara moral, tetapi juga memiliki dampak hukum yang harus dipertanggungjawabkan.

Dengan demikian, melindungi diri di ruang siber sejatinya adalah membekali anak untuk menjadi pribadi yang sadar, berhati-hati, beretika, terampil, dan bertanggung jawab. Bekal ini akan menumbuhkan resiliensi, membuat mereka mampu menghadapi ancaman, belajar dari pengalaman, dan tumbuh sebagai generasi yang cerdas serta tangguh dalam memanfaatkan teknologi.

Tahukah Anda

Catatan penting (TIDAK UNTUK DISAMPAIKAN KE MURID):

Contoh perundungan daring dalam bagian ini disajikan semata untuk pembelajaran. Pendidik dan orang tua perlu menegaskan bahwa perilaku tersebut berbahaya, melanggar norma, dan berdampak serius, agar anak belajar menghindari dan melindungi diri, bukan meniru.

Kasus Perundungan Ekstrim Tahun 2022

Pada Juli 2022, publik dikejutkan oleh kasus perundungan berat yang menimpa seorang anak berusia 11 tahun. Korban mengalami perundungan berlapis fisik, psikologis, bahkan seksual yang kemudian direkam dalam sebuah video berdurasi 50 detik. Rekaman itu menunjukkan korban dipaksa melakukan tindakan asusila, lalu video tersebut tersebar melalui WhatsApp dan media sosial.

Penyebaran video membuat korban mengalami goncangan psikologis yang sangat serius. Rasa malu, tekanan sosial, dan trauma mendalam membuat kondisi fisik korban memburuk: menolak makan, depresi, hingga akhirnya meninggal dunia setelah sempat dirawat di rumah sakit.

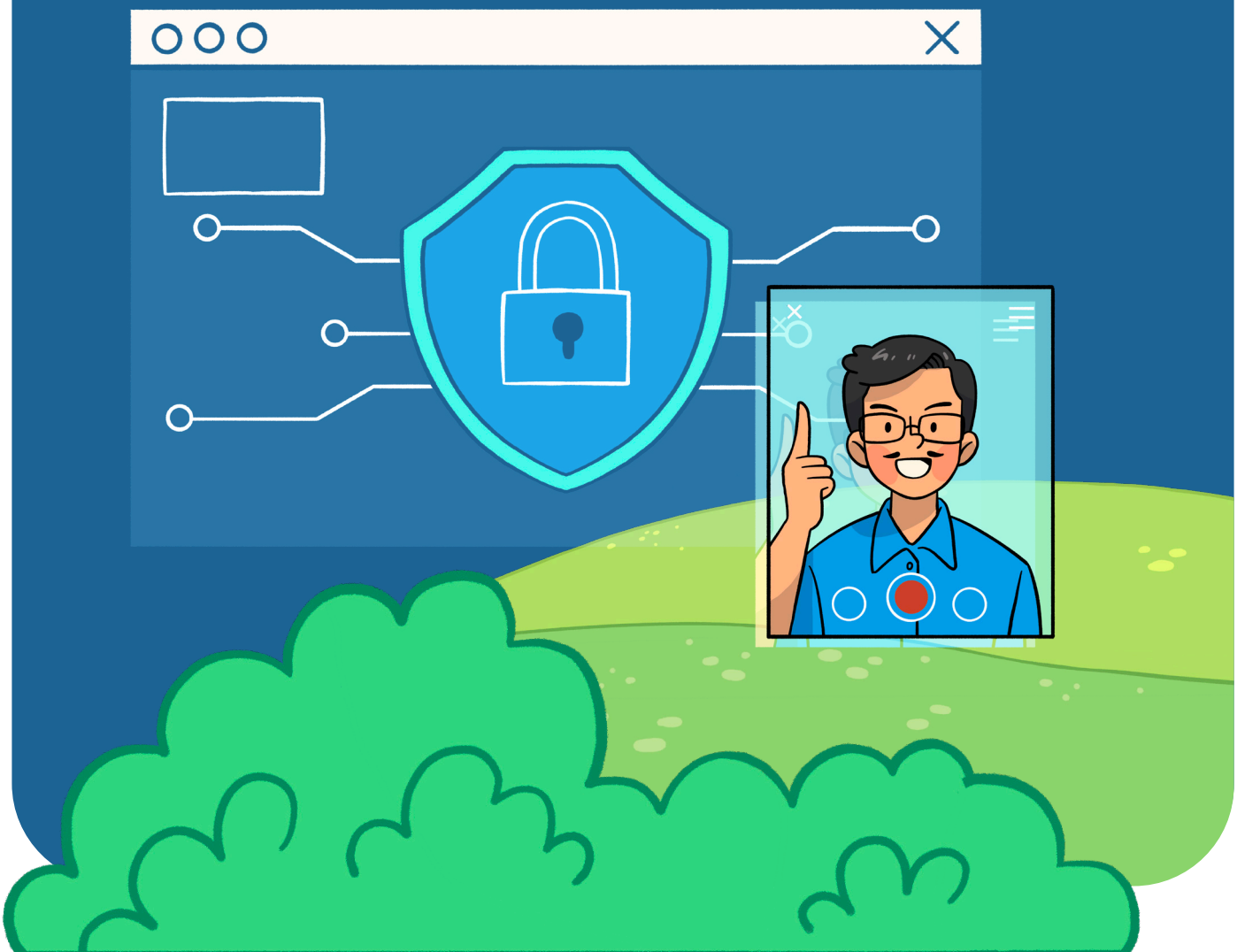
Komisi Perlindungan Anak Indonesia (KPAI) menilai kasus ini sebagai perundungan yang "berat dan kompleks," serta mendesak agar dibawa ke ranah hukum. Kepolisian Daerah Jawa Barat memeriksa setidaknya 15 orang terkait kasus tersebut, sementara pengamat anak menilai para pelaku (masih anak-anak) kemungkinan besar terpapar konten pornografi yang mendorong perilaku menyimpang.

Kasus ini menjadi contoh nyata betapa *cyberbullying* dapat melampaui batas sekadar ejekan atau komentar kasar di media sosial. Ketika tindakan perundungan terekam, tersebar, dan viral, dampak yang ditimbulkan bisa fatal hingga menghancurkan kesehatan mental korban, memengaruhi fisik, hingga merenggut nyawa.

Pelajaran penting: perundungan daring bukan hanya "kenakalan anak-anak" yang bisa dianggap remeh. Dampaknya nyata, berlapis, dan bisa berujung tragedi. Kasus yang terjadi di tahun 2022 menjadi pengingat keras bahwa setiap orang tua, pendidik, dan pemangku kebijakan perlu menempatkan pencegahan perundungan siber sebagai prioritas utama dalam melindungi anak-anak.

BAB
2

Pendidikan Keamanan Siber



BAB 2

Pendidikan Keamanan Siber

"Keamanan Siber adalah upaya adaptif dan inovatif untuk melindungi seluruh lapisan ruang siber, termasuk aset informasi yang ada di dalamnya, dari ancaman dan serangan siber, baik yang bersifat teknis maupun sosial."

(Peraturan Presiden Nomor 47 Tahun 2023 Tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber)

A Pendidikan Keamanan Siber: Mengapa Penting?

Rahman, et al. (2020) menyebutkan bahwa sangat penting melindungi anak-anak melalui pendidikan keamanan siber agar mereka dapat menyadari potensi risiko yang dihadapi ketika menggunakan alat komunikasi internet seperti media sosial, percakapan daring, dan gim daring. Kemudian Pantjawati (2021) menegaskan bahwa kesadaran dan pendidikan keamanan siber adalah inti dari segala upaya untuk mengamankan dunia siber. Altarawneh, et al. (2025) dalam jurnalnya *"Cybersecurity awareness among school students: Exploring influencing factors, legal implications, and knowledge gaps"* menyimpulkan bahwa pengajaran isu-isu keamanan siber dalam kurikulum sekolah memberikan kontribusi besar terhadap penyampaian pengetahuan mengenai perilaku aman di internet.

Peran pendidikan merupakan bagian kunci dari upaya keseluruhan untuk memperkuat kapasitas keamanan siber nasional dan dapat didefinisikan sebagai **"pengelolaan dan tata kelola program serta inisiatif pendidikan keamanan siber, serta keterjangkauan dan kesesuaiannya di seluruh lapisan masyarakat, termasuk peningkatan kesadaran, pembelajaran formal dan nonformal, jalur pelatihan vokasi dan profesional, serta pembangunan pengetahuan dan kemampuan melalui penelitian dan pengembangan."** *(A systems approach to understanding national cybersecurity education capacity, International Telecommunication Union, 2024)*

Pembangunan kapasitas keamanan siber mencakup tiga dimensi utama, yakni: mengembangkan kapasitas individu, memperkuat struktur kelembagaan, dan merancang kerangka kebijakan. Pendidikan keamanan siber dalam hal ini menjadi salah satu bentuk peningkatan kapasitas keamanan siber murid.

Mitigasi risiko di ruang siber

Pada Bab I sudah disampaikan berbagai bentuk ancaman siber yang dapat menyasar murid sebagai korbannya. Pendidikan keamanan siber akan meningkatan pengetahuan tentang ancaman siber tersebut dan berbagai langkah untuk melindungi diri di ruang siber sehingga secara tidak langsung diharapkan dapat menjadi bentuk mitigasi risiko bagi murid di ruang siber. Setelah mendapatkan materi pendidikan keamanan siber, murid diharapkan tidak menjagi korban kejahatan siber apalagi menjadi pelakunya.

Hak anak untuk dilindungi di ruang siber

Hak anak di ruang siber mencakup perlindungan dari eksploitasi dan konten negatif, hak untuk berpartisipasi dan berekspresi, serta pelindungan data pribadi yang didukung oleh regulasi seperti Konvensi Hak Anak (disahkan oleh Majelis Umum PBB pada 20 November 1989 dan sudah diratifikasi Indonesia melalui Keputusan Presiden Nomor 36 Tahun 1990) dan Peraturan Pemerintah Nomor 17 Tahun 2025 tentang Tata Kelola Penyelenggaraan Sistem Elektronik Dalam Pelindungan Anak (PP Tunas). Pelindungan ini juga melibatkan peningkatan literasi digital bagi anak dan orang tua, serta tanggung jawab Penyelenggara Sistem Elektronik (PSE) untuk menciptakan lingkungan digital yang aman dan mendukung tumbuh kembang anak. Melindungi hak anak di ruang siber bukan hanya menjadi kewajiban pemerintah dan PSE saja, tetapi perlu peran dari pendidik dan orang tua serta yang tidak kalah penting adalah kesediaan dari anak itu sendiri. Pendidikan keamanan siber di sekolah secara tidak langsung menjadi salah satu bentuk untuk melindungi hak anak di ruang siber.

Amanat pendidikan keamanan siber dalam Rencana Aksi Nasional Keamanan Siber 2024-2028 dan Peta Jalan Pelindungan Anak di Ranah Dalam Jaringan 2025-2029

Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2024 tentang Rencana Aksi Nasional Keamanan Siber Tahun 2024-2028 merupakan turunan dari Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. Rencana Aksi Nasional Keamanan Siber (RAN Kamsiber) adalah rencana aksi tingkat nasional yang berisi upaya terencana dan terukur untuk menjabarkan dan mengimplementasikan fokus area strategi keamanan siber nasional. Salah satu fokus area RAN Kamsiber yakni peningkatan kapabilitas, kapasitas, dan kualitas dengan salah satu sub-fokus areanya adalah pengembangan kurikulum

berkaitan dengan Keamanan Siber pada pendidikan anak usia dini, pendidikan dasar, pendidikan menengah, dan pendidikan tinggi.

Sementara itu, Peraturan Presiden Nomor 87 Tahun 2025 tentang Peta Jalan Pelindungan Anak di Ranah Dalam Jaringan Tahun 2025-2029 merupakan dokumen perencanaan pembangunan yang memuat panduan pelaksanaan pelindungan anak dari segala bentuk penyalahgunaan teknologi informasi dan komunikasi di ranah dalam jaringan. Peta Jalan ini dilaksanakan tidak hanya oleh kementerian/lembaga saja tetapi juga oleh pemerintah daerah provinsi dan pemerintah daerah kabupaten/kota. Berdasarkan Perpres ini, strategi pelindungan anak di ranah dalam jaringan terdiri dari pencegahan terjadinya dan penanganan penyalahgunaan teknologi informasi dan komunikasi serta kolaborasi peran pemangku kepentingan.

Pada strategi pencegahan, dengan fokus strategi pengurangan kerentanan, salah satu intervensi kuncinya adalah memperkuat substansi pelindungan anak di ranah dalam jaringan di satuan pendidikan dengan keluaran tersedianya modul dan terintegrasinya materi tentang pelindungan anak di ranah dalam jaringan ke dalam bahan ajar serta tersedianya pendidik dan tenaga kependidikan di satuan pendidikan yang memiliki pemahaman dalam pencegahan dan penanganan kekerasan anak di ranah dalam jaringan.

Terlaksananya pendidikan keamanan siber di satuan pendidikan menjadi implementasi amanat yang tertuang dalam Rencana Aksi Nasional Keamanan Siber 2024-2028 dan Peta Jalan Pelindungan Anak di Ranah Dalam Jaringan 2025-2029.

Pendidikan keamanan siber upaya menuju budaya keamanan siber

Budaya keamanan siber menjadi tujuan utama dari pendidikan keamanan siber. Pembelajaran materi keamanan siber yang sistematis diharapkan dapat mengembangkan keterampilan dalam menerapkan prinsip keamanan siber, tidak hanya saat pembelajaran bersama pendidik di sekolah, tetapi juga dalam kehidupan sehari-hari. Sehingga, dapat membentuk budaya keamanan siber murid kapanpun dan dimanapun berada, bahkan setelah lulus dari sekolah. Jika budaya keamanan siber sudah terbentuk dari sekolah tentunya akan membawa dampak positif bagi keamanan dan ketahanan siber nasional.

Pendidikan Keamanan Siber bukan hanya sebatas implementasi regulasi terkait tetapi menjadi langkah strategis membentuk budaya keamanan siber murid

B Pendidikan Keamanan Siber: Tujuan dan Prinsip Pelaksanaan

Pendidikan keamanan siber diselenggarakan dengan tujuan agar murid memiliki pengetahuan, sikap, dan perilaku yang mencerminkan budaya keamanan siber. Tujuan pendidikan ini mencakup tiga ranah utama:

1 Pengetahuan Keamanan Siber

Pengetahuan mencakup pemahaman murid tentang ancaman dan risiko siber, pelindungan data pribadi, pengelolaan informasi, jejak digital, etika dan perilaku digital, dasar-dasar kriptografi, serta peraturan perundang-undangan terkait ruang siber. Tahap ini bertujuan membekali murid dengan informasi faktual dan konsep teknis maupun etis sebagai landasan pengambilan keputusan yang aman di dunia digital.

2 Sikap Bijak di Ruang Siber

Sikap merujuk pada nilai, pandangan, dan kesadaran murid terhadap keamanan siber. Lingkupnya meliputi kepedulian, tanggung jawab etis dalam menjaga data pribadi, menghormati hak orang lain di internet, serta keberanian melaporkan ancaman jika ditemukan. Pendidikan keamanan siber tidak hanya mentransfer pengetahuan, tetapi juga membentuk kesadaran, nilai, dan prinsip yang mendorong murid untuk konsisten menerapkan perilaku aman.

3 Perilaku Aman di Ruang Siber

Perilaku merupakan wujud nyata penerapan pengetahuan dan sikap. Murid diharapkan memiliki keterampilan praktis, seperti membuat kata sandi yang kuat, mengaktifkan autentikasi ganda, tidak membagikan data pribadi sembarangan, menerapkan teknik kriptografi sederhana, serta menaati kebijakan sekolah terkait keamanan siber. Ranah ini menjadi indikator keberhasilan: murid bukan hanya tahu dan peduli, tetapi juga bertindak aman, etis, dan berkelanjutan di ruang siber.

Prinsip Implementasi: 7B dalam Pendidikan Keamanan Siber

Penerapan pendidikan keamanan siber di satuan pendidikan berlandaskan **prinsip 7B**: *Berbasis Data dan Fakta, Beraksi, Berempati, Berkembang, Berkelanjutan, Berkolaborasi,* dan *Berintegritas*. Seluruh prinsip ini saling melengkapi dan memberikan arah yang jelas bagi pendidik dalam membangun kompetensi keamanan siber yang menyeluruh.

Berbasis Data dan Fakta

Penyusunan materi dan metode pembelajaran didukung oleh sumber tepercaya sehingga informasi yang disampaikan akurat, mutakhir, dan bebas dari misinformasi. Prinsip ini memastikan bahwa proses belajar tidak menimbulkan bias maupun kesalahpahaman.

Beraksi

Pembelajaran tidak berhenti pada teori. Murid didorong untuk melakukan praktik nyata, baik secara individu maupun kelompok, agar terbentuk keterampilan digital yang dapat diterapkan langsung dalam kehidupan sehari-hari, seperti mengelola kata sandi atau melapor ketika menemukan konten tidak aman.

Berempati

Prinsip ini menekankan kemampuan murid dan pendidik untuk memahami perasaan dan perspektif orang lain di ruang siber. Empati menjadi fondasi penting untuk mencegah perundungan daring, ujaran kebencian, diskriminasi, dan penyebaran konten yang merugikan.

Berkembang

Ancaman siber terus berubah mengikuti perkembangan teknologi, termasuk munculnya *deepfake* dan kecerdasan buatan generatif. Karena itu, materi pembelajaran harus diperbarui secara berkala, dan pendidik perlu meningkatkan wawasan melalui referensi tambahan agar tetap relevan.

Berkelanjutan

Pendidikan keamanan siber memiliki sifat berjenjang dan saling terhubung antartingkat pendidikan. Sikap dasar yang ditanamkan sejak PAUD tetap relevan hingga SMA, sementara pemahaman tentang risiko berbagi data yang dipelajari di SMP akan memperkuat kesadaran keamanan siber di jenjang berikutnya.

Berkolaborasi

Keberhasilan pendidikan keamanan siber bergantung pada kolaborasi. Pendidik perlu bekerja sama dengan murid, orang tua, serta pemangku kepentingan lain agar pembelajaran bersifat dua arah, kontekstual, dan mendukung ekosistem belajar yang aman.

Berintegritas

Integritas menjadi bingkai dari seluruh prinsip lainnya. Semua pihak wajib bertindak sesuai aturan, nilai moral, dan etika digital. Kejujuran, keadilan, kepedulian, disiplin, dan tanggung jawab adalah nilai yang harus terus ditanamkan dalam setiap aktivitas belajar maupun praktik digital.

Dengan mengintegrasikan pengetahuan, sikap, dan perilaku dalam bingkai prinsip 7B, pendidikan keamanan siber diharapkan dapat menumbuhkan generasi yang HEBAT (Hati-hati, Etis, Bijak, Aman, dan Tangguh) di ruang siber.

C Kompetensi Pendidikan Keamanan Siber

Di era digital yang bergerak sangat cepat ini, kompetensi keamanan siber apa saja yang benar-benar fundamental dan harus dikuasai anak Indonesia?

Pertanyaan tersebut membawa substansi dan urgensi bahwa pendidikan keamanan siber di Indonesia memerlukan kerangka kompetensi yang komprehensif dan terstruktur. Hal ini menjadi salah satu prinsip fundamental dalam perancangan kerangka kompetensi pendidikan keamanan siber, yakni keselarasan dengan karakteristik dan tingkat perkembangan kognitif murid. Keseluruhannya mengindikasikan bahwa pendekatan pembelajaran dan materi yang disampaikan harus disesuaikan dengan usia, pemahaman, dan kapabilitas belajar murid pada setiap jenjang.

Penyusunan kerangka pada buku panduan ini menggunakan beberapa referensi utama sebagai acuan, khususnya dari aspek capaian pembelajaran dan penyelenggaraan pendidikan keamanan siber. Referensi ini mencakup standar internasional, praktik terbaik dari negara-negara lain yang telah maju dalam pendidikan keamanan siber, serta pedoman kurikulum yang relevan. Dengan demikian, kerangka yang dihasilkan diharapkan tidak hanya komprehensif dan relevan dengan konteks Indonesia, tetapi juga selaras dengan standar global dalam pendidikan keamanan siber.

Tabel 1 Daftar Referensi Acuan Pengembangan Kerangka Pendidikan Keamanan Siber

Referensi	Tahun	Kontekstualisasi
A Systematic Review of K-12 Cybersecurity Education	2019	▪ Praktik terbaik negara berkembang ▪ *Interdisciplinary* sesuai kurikulum tematik ▪ Asesmen sesuai sistem penilaian Indonesia ▪ *Teacher training* sesuai pengembangan pendidik
UK Council of Internet Safety - Education for a Connected World	2020	▪ Konsep diri dan Identitas: nilai Pancasila ▪ Interaksi Daring: nilai gotong royong ▪ Privasi dan Keamanan: kaidah UU Pelindungan Data Pribadi (PDP) ▪ Penjenjangan Usia: penjenjangan PAUD-SMA
Cyber.org K-12 Cybersecurity Learning Standards	2021	▪ *Digital Citizenship*: konsep warga negara digital dengan nilai Pancasila ▪ Konsep keamanan siber untuk pendidikan dasar dan menengah
SuperCyberKids Learning Framework	2023	▪ *Game-based learning* sesuai budaya bermain Indonesia ▪ Target usia 8-13 untuk SD-SMP ▪ *Hands-on learning* sesuai karakteristik pembelajaran Indonesia ▪ Kerangka pembelajaran holistik sesuai pendidikan karakter

Referensi tersebut selanjutnya dikontekstualisasikan dengan karakteristik anak di ruang siber dan kebijakan penyelenggaraan pendidikan di Indonesia. Karenanya, teridentifikasi lima elemen utama kompetensi keamanan siber yang saling berkaitan yaitu: **Kesadaran Keamanan Siber, Pelindungan Data Pribadi dan Jejak Digital, Etika & Perilaku Digital, Keterampilan Teknis Keamanan Siber dan Kesadaran Hukum di Ruang Siber.**

Tabel 2 Elemen Kompetensi Keamanan Siber

Elemen Kompetensi	Deskripsi
Kesadaran Keamanan Siber	Pemahaman terhadap ancaman dan risiko siber serta membangun kebiasaan melindungi diri di ruang siber. Topik-topik yang sesuai diantaranya: ▪ Pemahaman konsep dasar ancaman siber dan klasifikasi risiko ▪ Penerapan perilaku aman ▪ Identifikasi tingkat risiko dalam aktivitas digital
Pelindungan Data Pribadi & Jejak Digital	Pemahaman terhadap jenis-jenis data pribadi, mengelola informasi yang dibagikan, serta menyadari bahwa setiap aktivitas di ruang siber meninggalkan jejak digital yang memiliki konsekuensi. Topik-topik yang sesuai diantaranya: ▪ Pengenalan jenis data pribadi dan karakteristik sensitif data ▪ Pengaturan hak akses dan pengaturan privasi ▪ Manajemen identitas daring
Etika & Perilaku Digital	Kemampuan berinteraksi secara bertanggung jawab di ruang siber, antara lain dengan bersikap sopan, menghargai hak orang lain, dan menolak perilaku merugikan seperti penyebaran informasi tidak benar atau perundungan daring. Topik-topik yang sesuai diantaranya: ▪ Penerapan prinsip consent dalam berbagi data dan konten ▪ Identifikasi dan pencegahan perundungan daring ▪ Produksi konten positif dan penghormatan hak cipta
Keterampilan Teknis Keamanan Siber	Kemampuan menerapkan perilaku aman di ruang siber dan pemahaman terhadap konsep dasar kriptografi serta penerapannya dalam mengamankan perangkat, akun, dan data. Topik-topik yang sesuai diantaranya: ▪ Penggunaan kata sandi kompleks dan sistem autentikasi ganda (*2 Factor Authentication*) ▪ Penggunaan enkripsi dasar pada file/pribadi ▪ Verifikasi kebenaran informasi dan pelaporan insiden siber

Elemen Kompetensi	Deskripsi
Kesadaran Hukum di Ruang Siber	Pemahaman terhadap peraturan perundang-undangan terkait ruang siber, antara lain informasi dan transaksi elektronik, hak cipta, privasi, dan pelindungan data. Topik-topik yang sesuai diantaranya: ▪ Pengetahuan hak dan kewajiban pengguna sesuai UU ITE dan UU PDP ▪ Pemahaman sanksi atas penyalahgunaan penggunaan teknologi ▪ Kepatuhan pada aturan di ruang siber

D Kompetensi Pendidikan Keamanan Siber sesuai Jenjang (PAUD, SD, SMP, SMA/SMK)

Jenjang PAUD

Pada jenjang PAUD, murid berada pada tahap eksplorasi awal terhadap teknologi digital. Pendekatan yang digunakan bersifat protektif dengan penekanan pada pendampingan orang dewasa dan pembentukan kebiasaan dasar yang aman.

Elemen	Kompetensi
1. Kesadaran Keamanan Siber	Murid memahami bahwa penggunaan perangkat teknologi harus dengan pendampingan orang tua/wali atau pendidik
2. Pelindungan Data Pribadi & Jejak Digital	Murid dapat mengidentifikasi informasi pribadi dasar
3. Etika & Perilaku Digital	Murid mengetahui perilaku aman saat menggunakan perangkat teknologi
	Murid mengetahui perilaku aman saat berkomunikasi secara daring
4. Keterampilan Teknis Keamanan Siber	Murid dapat menolak permintaan informasi pribadi

Jenjang SD

Murid SD mulai mengembangkan kemampuan kognitif untuk memahami konsep abstrak secara sederhana. Pada jenjang ini, pendekatan menggunakan pembelajaran berbasis pengalaman konkret dan observasi langsung dengan pengenalan aturan yang jelas dan konsisten.

Elemen	Kompetensi
1. Kesadaran Keamanan Siber	Murid mengidentifikasi aplikasi dan konten di ruang siber sesuai usia
	Murid mengikuti aturan penggunaan perangkat digital dan internet
2. Pelindungan Data Pribadi & Jejak Digital	Murid memahami pengelolaan data pribadi dan batasan berbagi informasi
	Murid memahami konsekuensi jejak digital
3. Etika & Perilaku Digital	Murid memahami berbagai bentuk perilaku merugikan di ruang siber
	Murid memahami perilaku yang menghormati privasi
	Murid memahami bahwa membagikan informasi yang belum pasti kebenarannya bisa merugikan orang lain
	Murid memahami perundungan siber dan tahu cara melapor
4. Keterampilan Teknis Keamanan Siber	Murid dapat mengkomunikasikan situasi yang tidak aman di ruang siber kepada orang tua/wali atau pendidik
	Murid dapat menerapkan pengamanan pada perangkat teknologi
	Murid dapat mengidentifikasi ciri-ciri informasi yang meragukan
	Murid memahami penggunaan kata sandi
5. Kesadaran Hukum di Ruang Siber	Murid mengetahui aturan dasar terkait ruang siber

Jenjang SMP

Pada jenjang SMP, murid memasuki masa formal *operational thinking* awal dan mulai mengembangkan kemampuan berpikir analitis. Mereka dapat memahami konsep sebab-akibat yang lebih kompleks dan mulai mengembangkan kemandirian dalam pengambilan keputusan digital.

Elemen	Kompetensi
1. Kesadaran Keamanan Siber	Murid dapat mengelola waktu penggunaan perangkat teknologi digital
	Murid dapat mengidentifikasi jenis-jenis ancaman siber
	Murid dapat mengidentifikasi permintaan informasi pribadi pada penggunaan aplikasi atau platform daring
2. Pelindungan Data Pribadi & Jejak Digital	Murid memahami risiko membagikan informasi pribadi di ruang siber
	Murid dapat menganalisis dampak jejak digital terhadap reputasi pribadi
3. Etika & Perilaku Digital	Murid menunjukkan perilaku etis dalam berinteraksi di ruang siber untuk membangun ekosistem yang aman dan sehat
	Murid memahami konsep persetujuan (*consent*) di ruang siber
	Murid dapat menganalisis dampak sosial penyebaran konten negatif dan berperan aktif melakukan pencegahan
	Murid dapat menjelaskan bentuk dan dampak perundungan siber serta dapat mempraktikkan langkah pelindungan untuk melindungi diri dan orang lain

4. Keterampilan Teknis Keamanan Siber	Murid dapat menyusun laporan kejahatan siber serta melaporkan kepada orang tua/wali atau pendidik
	Murid dapat menerapkan pengaturan keamanan dan privasi pada perangkat dan akun digital yang digunakan di bawah bimbingan orang tua/wali
	Murid menerapkan verifikasi kebenaran informasi
	Murid memahami peran kriptografi dalam kehidupan sehari-hari
5. Kesadaran Hukum di Ruang Siber	Murid mengetahui aturan hukum dasar terkait aktivitas daring remaja
	Murid memahami keterkaitan antara perilaku daring yang aman dan kepatuhan hukum

Jenjang SMA/SMK

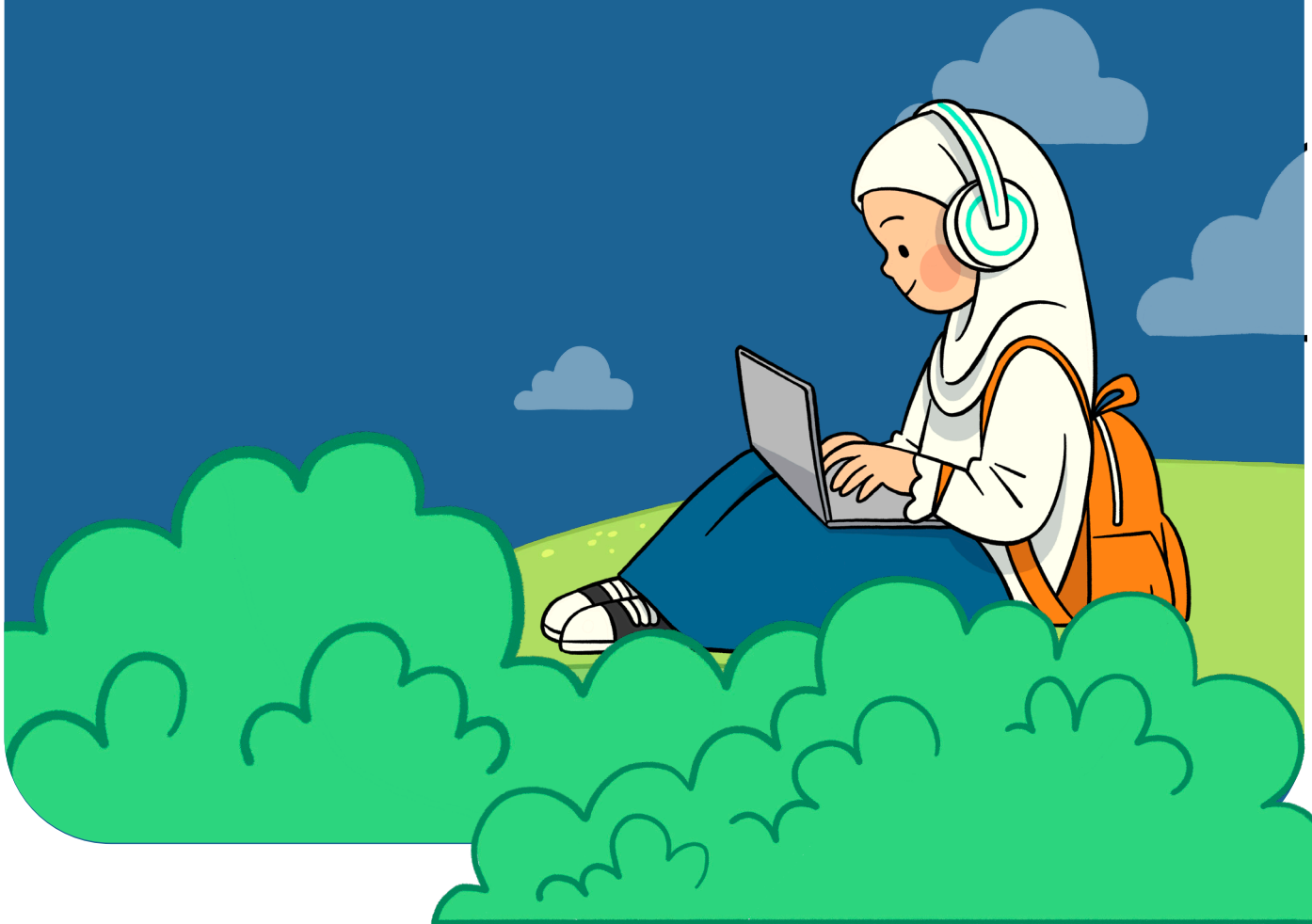
Murid SMA/SMK telah mengembangkan kemampuan berpikir abstrak dan analitis yang lebih matang. Mereka diharapkan dapat mengimplementasikan kompetensi keamanan siber secara mandiri dan menjadi agen positif dalam ekosistem digital.

Elemen	Kompetensi
1. Kesadaran Keamanan Siber	Murid dapat mengatur penggunaan media sosial dan internet secara produktif dan sehat
	Murid dapat mengidentifikasi dan mencegah risiko siber
	Murid dapat menganalisis risiko pembuatan akun pada platform digital
2. Pelindungan Data Pribadi & Jejak Digital	Murid memahami hak dan tanggungjawab atas data pribadi pihak lain yang sedang ia pegang
	Murid dapat memahami prinsip manajemen identitas daring
	Murid dapat menerapkan langkah-langkah menjaga citra positif

3. Etika & Perilaku Digital	Murid dapat mengevaluasi perilaku di ruang siber sesuai etika digital
	Murid dapat mengidentifikasi konflik digital dan memilih interaksi yang aman
	Murid dapat memproduksi dan menyebarkan konten perilaku positif
	Murid dapat menerapkan langkah-langkah pencegahan dan penanganan perundungan siber
4. Keterampilan Teknis Keamanan Siber	Murid dapat menyampaikan laporan insiden siber
	Murid dapat menerapkan dan menilai langkah pengamanan perangkat dan akun
	Murid dapat membedakan opini, fakta, dan propaganda
	Menerapkan teknik enkripsi dasar
5. Kesadaran Hukum di Ruang Siber	Murid dapat menjelaskan hubungan regulasi siber, hak digital, dan kewajiban hukum
	Murid dapat menganalisis pelanggaran siber dan jenis-jenisnya

BAB
3

Implementasi Pendidikan Keamanan Siber dalam Kebijakan dan Budaya Sekolah



BAB 3

Implementasi Pendidikan Keamanan Siber dalam Kebijakan dan Budaya Sekolah

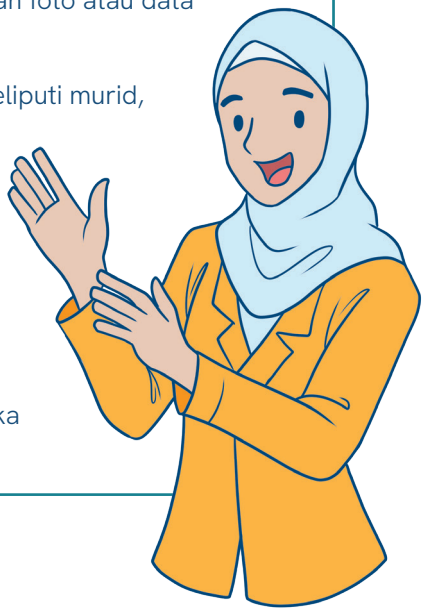
A Budaya Keamanan Siber: Seperti Apakah Itu?

Sama seperti kompetensi lainnya, kompetensi keamanan siber tidak cukup hanya diajarkan dalam bentuk teori. Tapi juga dibutuhkan internalisasi, penghayatan, dan kesempatan untuk menerapkan pengetahuan yang diperoleh dalam keseharian di ruang siber. Karenanya, pelaksanaan pendidikan keamanan siber membutuhkan ekosistem yang mendukung, agar kebiasaan aman berteknologi dapat berkembang secara alami bagi para murid.

Kata Kunci

Budaya Keamanan Siber dapat didefinisikan sebagai sistem nilai, kebiasaan, dan perilaku yang didasarkan pada kesadaran akan risiko di ruang siber, serta komitmen bersama untuk melindungi diri dan lingkungan dari ancaman siber. Budaya ini juga mencakup kesadaran untuk menjaga jejak digital yang positif, serta etika berbagi informasi (seperti meminta persetujuan sebelum mengunggah foto atau data orang lain).

Budaya ini terbentuk ketika seluruh warga sekolah, yang meliputi murid, pendidik, tenaga kependidikan, hingga pimpinan sekolah, mampu memahami berbagai ancaman di ruang siber seperti pencurian data pribadi, peretasan akun, maupun penipuan daring, dan menjadikan perilaku aman sebagai standar bersama. Perilaku aman ini tidak hanya bersifat teknis, tetapi juga mencakup aspek kepatuhan terhadap kebijakan penggunaan teknologi sekolah serta sikap proaktif (seperti berinisiatif melakukan pelaporan insiden jika menemukan potensi ancaman keamanan).



Sebagai negara dengan tingkat penggunaan internet yang sangat tinggi, budaya keamanan siber di Indonesia menjadi kebutuhan mendesak. Pembentukan budaya keamanan siber yang efektif memerlukan pendekatan holistik. Studi Ibrahim dkk. (2024) menunjukkan bahwa **pendidikan keamanan siber di jenjang K-12 lebih berhasil ketika kurikulum dikombinasikan dengan praktik nyata, fasilitas pendukung, dan kebijakan institusi yang konsisten.** Praktik nyata tersebut dapat diwujudkan melalui langkah-langkah konkret dalam keseharian, misalnya membiasakan diri mengunci akun atau perangkat saat tidak digunakan, serta selalu memejriksa izin akses aplikasi sebelum mengunduh atau menggunakannya.

Dengan demikian, budaya keamanan siber tidak dapat dibangun hanya melalui instruksi teknis semata, melainkan melalui sinergi kebijakan, pembelajaran, infrastruktur, dan partisipasi komunitas pendidikan secara berkelanjutan.

Peran Pimpinan Satuan Pendidikan dalam Membangun Budaya Keamanan Siber

Ancaman siber sering dipersepsikan sebagai isu teknis yang rumit dan sulit dikendalikan. Namun, satuan pendidikan justru dapat menjadi garis pertahanan pertama melalui kepemimpinan yang terarah. **Pimpinan satuan pendidikan** memiliki peran sentral dalam membentuk budaya keamanan siber, karena setiap kebijakan, arahan, dan teladan yang ditetapkan akan memengaruhi pola pikir dan perilaku seluruh warga sekolah.

Kepemimpinan yang efektif ditunjukkan melalui kemampuan menetapkan prioritas keamanan siber dalam tata kelola sekolah, misalnya dengan memastikan kurikulum dan kegiatan pembelajaran memuat literasi keamanan siber yang relevan, serta membangun lingkungan yang mendukung praktik aman dalam penggunaan teknologi. Selain itu, pimpinan satuan pendidikan berperan menggerakkan partisipasi pendidik, staf, murid, dan orang tua untuk bersama-sama menjaga keamanan siber.

Fokus kepemimpinan tidak semata-mata pada risiko atau ancaman, tetapi juga pada optimalisasi aset yang telah dimiliki sekolah. Kapasitas pendidik dalam membimbing murid, kedisiplinan murid, dukungan dari orang tua, serta fasilitas teknologi yang tersedia dapat menjadi modal awal. Pendekatan **Pengembangan Komunitas Berbasis Aset (PKBA)** memberikan kerangka untuk mengoptimalkan potensi tersebut agar terbentuk ekosistem digital yang aman dan berkelanjutan (Kretzmann & McKnight, 2010).

Kata Kunci

PKBA adalah pendekatan yang menekankan pada kekuatan, potensi, dan sumber daya yang sudah dimiliki oleh komunitas, bukan pada kekurangannya. Dalam konteks pendidikan keamanan siber, konsep ini sangat relevan karena membantu pimpinan satuan pendidikan membangun budaya keamanan siber dari dalam lingkungan sekolah sendiri.

Melalui PKBA, sekolah dapat mengidentifikasi dan memanfaatkan aset yang sudah ada. Misalnya guru yang melek digital, siswa yang kreatif, atau orang tua yang peduli pada keamanan anak di internet sebagai penggerak perubahan.

Dengan cara ini, pembiasaan perilaku aman di ruang siber tidak hanya datang dari aturan atau pelatihan formal, tetapi tumbuh secara alami melalui partisipasi bersama.

Selain penguatan aset, kepemimpinan juga mencakup pembangunan **budaya kolaboratif**. Pimpinan satuan pendidikan dapat menjalin kemitraan dengan berbagai komunitas, lembaga pemerintah, atau pihak swasta untuk memperkaya sumber daya pembelajaran, menghadirkan pelatihan bagi pendidik, serta menambah akses pada perangkat dan sistem keamanan yang memadai. Dengan cara ini, sekolah tidak hanya bergantung pada kemampuan internal, tetapi juga terbuka terhadap dukungan eksternal.

Kepemimpinan yang konsisten dalam membangun budaya keamanan siber akan menghasilkan dampak jangka panjang. Murid tidak hanya terlindungi dari ancaman siber, tetapi juga memiliki keterampilan kritis untuk menghadapi risiko siber di luar sekolah. Pada akhirnya, **satuan pendidikan dapat berperan sebagai pusat pembelajaran sekaligus teladan dalam penerapan budaya keamanan siber di masyarakat**.

Strategi untuk Membentuk dan Meningkatkan Budaya Keamanan Siber di Satuan Pendidikan

Budaya keamanan siber di satuan pendidikan tidak hanya dibangun melalui kebijakan teknis, tetapi juga melalui keterlibatan seluruh warga sekolah. Oleh karena itu, strategi penguatan budaya ini perlu dilakukan secara terpadu, berkelanjutan, dan kolaboratif. Berikut ini adalah beberapa strategi yang dapat dilakukan oleh satuan pendidikan untuk membentuk dan meningkatkan budaya keamanan siber di lingkungannya.

Tabel 3 Strategi untuk Membentuk dan Meningkatkan Budaya Keamanan Siber di Satuan Pendidikan

Area Strategi	Contoh Implementasi
Penguatan Literasi Digital	▪ Memberikan edukasi rutin bagi pendidik, murid, staf, dan orang tua tentang praktik aman di dunia digital. ▪ Memasukkan topik keamanan siber dalam kurikulum atau kegiatan ekstrakurikuler.
Penerapan Kebijakan Keamanan Siber Sekolah	▪ Menggunakan akun resmi sekolah untuk kegiatan administrasi dan pembelajaran. ▪ Mengatur penggunaan Wi-Fi sekolah agar hanya dapat diakses oleh pihak berwenang. ▪ Membuat aturan yang jelas tentang penggunaan perangkat digital di lingkungan sekolah.
Penerapan Praktik Aman Sehari-hari	▪ Rutin memperbarui perangkat dan aplikasi di laboratorium komputer maupun perangkat pendidik. ▪ Melatih murid dan pendidik agar tidak sembarangan mengunduh aplikasi atau membuka tautan yang mencurigakan. ▪ Menjaga kerahasiaan data pribadi murid, pendidik, dan staf sekolah.
Kolaborasi dengan Orang Tua dan Komunitas	▪ Mengajak orang tua mendampingi anak dalam penggunaan perangkat dan internet di rumah agar digunakan secara bijak dan sesuai dengan usia (termasuk dalam hal pembatasan durasi penggunaan *perangkat/screen time*, seperti pembatasan penggunaan gawai saat makan). ▪ Mengadakan seminar atau *workshop* bersama berbagai komunitas tentang ancaman dan solusi keamanan siber. ▪ Membentuk tim keamanan siber yang terdiri dari perwakilan pendidik, murid, staf, dan orang tua untuk mengawal kebijakan keamanan siber sekolah. ▪ Menyusun berbagai program sekolah yang mengintegrasikan aspek keamanan siber (Rencana Kerja Tahunan/RKT, Rencana Kegiatan Anggaran Sekolah/RKAS, dan Kurikulum Satuan Pendidikan/KSP) dengan pendampingan dari pengawas.

Area Strategi	Contoh Implementasi
Evaluasi dan Peningkatan Berkelanjutan	▪ Melakukan audit keamanan sistem dan jaringan sekolah secara berkala. ▪ Mengevaluasi efektivitas program literasi dan kebijakan yang diterapkan. ▪ Menyusun laporan keamanan siber tahunan sebagai bentuk akuntabilitas dan perbaikan berkelanjutan.
Kolaborasi dengan Praktisi atau Organisasi yang Relevan	▪ Mengundang guru tamu dari Badan Siber dan Sandi Negara, Kementerian Komunikasi dan Digital, dan sebagainya. ▪ Bedah kasus kejahatan siber dengan mengundang pihak Kepolisian, Kejaksaan, atau Peradilan. ▪ Sesi diskusi terkait implementasi pelindungan anak di ruang siber dengan organisasi penggiat keamanan siber. ▪ Bekerja sama dengan Tim Tanggap Insiden Siber (TTIS) untuk menangani berbagai macam kasus siber yang ditemukan, terutama yang bersifat kompleks.

Dengan strategi ini, satuan pendidikan bukan hanya mampu melindungi data dan sistem dari ancaman digital, tetapi juga menumbuhkan budaya keamanan siber yang kuat di kalangan murid, pendidik, orang tua, dan komunitas sekolah.

B Budaya Keamanan Siber: Kolaborasi dan Tanggung Jawab Bersama

Untuk mewujudkan budaya keamanan siber yang berkelanjutan, diperlukan komitmen, kesadaran, dan kontribusi aktif dari setiap individu. Berikut ini adalah peran strategis yang dapat dijalankan oleh setiap unsur warga sekolah untuk menciptakan budaya keamanan siber demi tercapainya lingkungan yang aman, responsif, dan beretika.

Tabel 4 Inspirasi Peran Aktif dan Kolaborasi dalam Mewujudkan Budaya Keamanan Siber

Warga Sekolah	Peranan yang Dapat Diambil
Kepala Sekolah	▪ Mendorong pengembangan program dan fasilitas ramah siber melalui kebijakan satuan pendidikan, termasuk mendukung penggunaan teknologi secara bijak dan sesuai dengan usia (termasuk dari segi durasi penggunaan perangkat/*screen time*). ▪ Mendukung peningkatan kapasitas pendidik. ▪ Mengembangkan kemitraan dengan lembaga atau instansi lain (seperti Tim Tanggap Insiden Siber/TTIS) untuk melaksanakan aksi keamanan siber dan penanganan kasus siber yang lebih kompleks.
Pengawas Sekolah	▪ Mendampingi satuan pendidikan dalam penyusunan program sekolah (Rencana Kerja Tahunan/RKT, Rencana Kegiatan Anggaran Sekolah/RKAS, dan Kurikulum Satuan Pendidikan/KSP) agar mengintegrasikan aspek keamanan siber. ▪ Memberikan pendampingan kepada sekolah saat penyusunan Kurikulum Satuan Pendidikan/KSP di awal tahun ajaran untuk memastikan kebijakan keamanan siber terakomodasi.
Pendidik	▪ Menyisipkan materi-materi keamanan siber dalam pembelajaran. ▪ Melakukan pembiasaan ramah siber di kelas (misalnya mematikan perangkat setelah digunakan dan menggunakan perangkat dengan batasan durasi tertentu). ▪ Berkomunikasi dengan orang tua tentang isu keamanan siber. ▪ Melakukan pemantauan aktif jika terjadi kasus kekerasan di ruang siber (*cyberbullying*).

Warga Sekolah	Peranan yang Dapat Diambil
Pendidik Informatika	▪ Ikut aktif memetakan risiko siber di lingkungan satuan pendidikan. ▪ Mengembangkan dan melatih skenario penanganan gangguan keamanan siber di sekolah (misalnya, sistem peringatan dini ketika terdapat indikasi kebocoran data atau disinformasi) ▪ Mengedukasi staf dan murid mengenai pentingnya kebijakan keamanan siber (termasuk pengelolaan kata sandi yang kuat dan aman). ▪ Melakukan pemantauan aktif jika terjadi kasus kekerasan di ruang siber (*cyberbullying*). ▪ Bekerja sama dengan kepala sekolah dan pihak lain (seperti Tim Tanggap Insiden Siber/TTIS) untuk penanganan kasus siber yang lebih kompleks.
Tenaga Kependidikan	▪ Memastikan penggunaan perangkat dan perangkat lunak yang aman di seluruh satuan pendidikan (termasuk pembaruan sistem keamanan dan perangkat lunak antivirus). ▪ Mengelola sistem penyimpanan data yang aman dan sesuai dengan kebijakan pelindungan data pribadi (misalnya enkripsi data). ▪ Melakukan pemantauan aktif jika terjadi kasus kekerasan di ruang siber (*cyberbullying*).
Pustakawan	▪ Menambah koleksi perpustakaan dengan sumber belajar yang terkait keamanan siber. ▪ Memberikan sorotan untuk sumber belajar terkait isu keamanan siber di perpustakaan (misal: membuat ‘pojok siber aman’). ▪ Melakukan pemantauan aktif jika terjadi kasus kekerasan di ruang siber (*cyberbullying*).
Murid	▪ Mematuhi aturan atau kesepakatan yang berlaku terkait penggunaan perangkat. ▪ Membangun kesadaran akan pentingnya keamanan siber. ▪ Ikut aktif dalam pemantauan di satuan pendidikan (penggunaan kata sandi yang kuat, perangkat yang aman, dll). ▪ Mendampingi teman sebaya dalam kegiatan terkait keamanan siber. ▪ Menjadi agen keamanan siber (kamsiber).

Warga Sekolah	Peranan yang Dapat Diambil
Komite Sekolah	▪ Bekerja sama dengan pimpinan satuan pendidikan untuk mendukung penerapan kebijakan keamanan siber di sekolah. ▪ Menyediakan dukungan dan masukan untuk melaksanakan pelatihan keamanan siber bagi pendidik, staf, dan murid. ▪ Mengembangkan kemitraan dengan lembaga atau organisasi eksternal untuk mendukung program keamanan siber dan pelindungan data di lingkungan sekolah.
Keluarga	▪ Mengedukasi anak-anak mengenai pentingnya menjaga privasi dan keamanan data pribadi di ruang siber (misalnya, tidak membagikan informasi pribadi sembarangan). ▪ Menggunakan perangkat yang aman dengan memastikan pengaturan privasi dan kontrol orang tua di perangkat yang digunakan anak-anak. ▪ Mendorong penggunaan internet yang sehat dan aman, termasuk memberikan batasan untuk durasi penggunaan perangkat/*screen time* (disesuaikan dengan usia). ▪ Menerapkan aturan zona tanpa gawai di rumah (misalnya saat makan bersama). ▪ Membimbing anak-anak dalam mengenali potensi ancaman siber (seperti kejahatan siber, perundungan siber, dll). ▪ Mendukung penerapan kebijakan keamanan siber yang ada di sekolah dan terlibat dalam pelatihan atau diskusi yang diadakan oleh sekolah mengenai keamanan siber.
Komunitas	▪ Mendukung dan berkolaborasi dengan satuan pendidikan untuk menciptakan kesadaran bersama tentang pentingnya keamanan siber di lingkungan sekolah dan sekitarnya. ▪ Menyediakan pelatihan dan *workshop* keamanan siber untuk warga sekolah, termasuk orang tua dan murid, agar mereka lebih memahami cara melindungi diri dari ancaman siber. ▪ Membantu mengedukasi masyarakat sekitar tentang bahaya dunia maya dan cara-cara untuk tetap aman berinteraksi di internet, seperti cara menghindari kejahatan siber, serta pelindungan data pribadi. ▪ Membantu satuan pendidikan dalam menciptakan dan menerapkan kebijakan keamanan siber yang sesuai dengan kebutuhan lokal dan perkembangan teknologi.

C Membangun Budaya Keamanan Siber melalui Kurikulum Satuan Pendidikan (KSP)

Pendidikan merupakan garda terdepan dalam membangun fondasi ketahanan bangsa, termasuk di ruang siber. Integrasi prinsip-prinsip keamanan siber ke dalam Kurikulum Satuan Pendidikan (KSP) bukan hanya sebuah inovasi pedagogis, melainkan sebuah keharusan strategis untuk mempersiapkan generasi muda yang cakap, kritis, dan bertanggung jawab dalam ruang siber. Pendekatan melalui kurikulum memastikan bahwa pembangunan budaya keamanan siber dilakukan secara sistematis, terstruktur, dan berkelanjutan, menjangkau seluruh murid pada semua jenjang.

Integrasi keamanan siber dalam KSP dapat dimulai dari **analisis karakteristik satuan pendidikan**. Setiap sekolah memiliki latar belakang yang berbeda, baik dari sisi murid, pendidik, tenaga kependidikan, maupun ketersediaan sarana prasarana dan dukungan sosial-budaya. Analisis ini menjadi dasar untuk merumuskan visi, misi, dan tujuan yang relevan dengan kebutuhan lokal, sekaligus menanamkan nilai-nilai keamanan siber dalam profil lulusan. Dengan demikian, kompetensi yang dihasilkan tidak hanya berupa penguasaan akademik, tetapi juga karakter tangguh dalam menghadapi risiko siber, sesuai dengan delapan dimensi profil lulusan.

Selanjutnya, pengorganisasian pembelajaran dalam KSP memberi ruang untuk memasukkan materi keamanan siber melalui jalur intrakurikuler, kokurikuler, maupun ekstrakurikuler.

1. Intrakurikuler	Pada jalur intrakurikuler, topik keamanan siber dapat disisipkan dalam mata pelajaran yang relevan (dilihat dari capaian pembelajaran dan tujuan pembelajarannya). Sebagai contoh, mata pelajaran Informatika dapat berfokus pada teknis keamanan akun dan pengelolaan data, sedangkan mata pelajaran Pendidikan Pancasila dapat menekankan pada aspek hak digital, etika, dan tanggung jawab warga negara di ruang siber.
2. Kokurikuler	Pada kegiatan kokurikuler, sekolah dapat mengembangkan proyek atau diskusi lintas mata pelajaran yang mengangkat isu-isu nyata di ruang siber.
3. Ekstrakurikuler	Kegiatan ekstrakurikuler keamanan siber dapat dikembangkan melalui klub, proyek, atau kegiatan kolaboratif yang memperluas minat dan kepedulian murid. Namun, jika sumber daya yang dimiliki terbatas, satuan pendidikan dapat mengintegrasikan kompetensi keamanan siber ke dalam berbagai kegiatan ekstrakurikuler yang sudah ada, sehingga lebih fleksibel, efisien, dan mudah dijalankan oleh sekolah.

Pendekatan seperti ini menjamin bahwa pembangunan budaya aman siber berlangsung menyeluruh dan berkelanjutan. Selain kurikulum, dukungan kebijakan teknis yang tegas juga diperlukan, seperti pengaturan akses Wi-Fi yang aman dan penerapan penyaringan konten (*filtering*) untuk melindungi murid dari paparan informasi negatif.

Selain itu, sekolah juga perlu merumuskan strategi untuk prosedur penanganan atau pemberian konsekuensi bagi kasus pelanggaran keamanan siber. Pendekatan ini tidak sekadar memberi sanksi, melainkan berfokus pada aspek edukatif dan perbaikan perilaku, agar murid memahami konsekuensi dari tindakannya dan tidak mengulanginya di masa depan.

D Penyusunan Kurikulum Satuan Pendidikan (KSP) yang Membangun Budaya Keamanan Siber

Membangun budaya keamanan siber tidak dapat dilakukan secara instan, keamanan siber adalah isu yang semakin relevan seiring berkembangnya dunia digital. Dalam menghadapi tantangan ini, sekolah berperan penting dalam membentuk karakter murid yang tidak hanya terampil dalam menggunakan teknologi, tetapi juga memiliki kesadaran yang tinggi akan pentingnya pelindungan data dan informasi pribadi. Untuk itu, pendidikan keamanan siber perlu dijadikan bagian dari kurikulum yang terintegrasi, dimulai sejak jenjang pendidikan dasar. Melalui kurikulum ini, murid tidak hanya belajar cara menggunakan teknologi, tetapi juga memahami risiko yang menyertainya dan bagaimana menghadapinya dengan bijak.

Untuk memastikan penerapan yang efektif, pengembangan Kurikulum Satuan Pendidikan (KSP) menjadi kunci dalam menciptakan lingkungan belajar yang mendukung pembelajaran tentang keamanan siber. Hal ini penting untuk dilakukan oleh satuan pendidikan guna memastikan bahwa pendidikan yang diberikan memenuhi standar kualitas yang relevan dengan kebutuhan zaman. Setiap satuan pendidikan memiliki konteks yang unik, baik dari segi latar belakang sosial-ekonomi-budaya, situasi geografis, maupun karakteristik murid dan pendidiknya. Oleh karena itu, kurikulum untuk keamanan siber perlu dirancang sedemikian rupa agar sesuai dengan kebutuhan dan kondisi lokal masing-masing sekolah, sekaligus memberikan hasil pembelajaran yang optimal.

Dalam pengembangan KSP untuk keamanan siber, sekolah perlu mengawalinya dengan melakukan **refleksi dan analisis terhadap kondisi yang ada di satuan pendidikan**, termasuk kesiapan teknologi, kesadaran akan ancaman siber, serta infrastruktur pendukung. Sumber data utama KSP adalah **rapor pendidikan** dan **hasil pemetaan pemanfaatan teknologi** yang mencakup penggunaan perangkat, perangkat lunak, dan kebijakan keamanan yang sudah diterapkan di sekolah.

Selain itu, **pemetaan terhadap potensi risiko siber** yang mungkin dihadapi oleh murid dan staf juga perlu dilakukan oleh satuan pendidikan. Hal ini mencakup analisis ancaman terhadap data pribadi, pemahaman tentang perilaku yang aman di ruang siber, serta langkah mitigasi yang dapat diambil oleh sekolah untuk mengurangi potensi bahaya. Proses ini perlu dilakukan secara kolaboratif dengan melibatkan seluruh warga sekolah, termasuk murid, pendidik, dan orang tua, guna memastikan bahwa kebijakan dan praktik yang dikembangkan sesuai dengan tantangan yang ada.

Berdasarkan panduan KSP, terdapat empat komponen utama yang perlu dipertimbangkan dalam merancang dan melaksanakan pendidikan yang berkualitas:

1. **Analisis karakteristik satuan pendidikan**	Memahami kondisi dan kebutuhan unik dari setiap satuan pendidikan.
2. **Visi, misi, dan tujuan**	Pada kegiatan kokurikuler, sekolah dapat mengembangkan proyek atau diskusi lintas mata pelajaran yang mengangkat isu-isu nyata di ruang siber.
3. **Pengorganisasian pembelajaran**	Menyusun struktur pembelajaran yang mendukung pengembangan kompetensi keamanan siber.
4. **Perencanaan pembelajaran**	Merancang langkah-langkah konkret untuk mengintegrasikan keamanan siber dalam setiap aspek pembelajaran.

Program-program terkait Pendidikan Keamanan Siber dapat diintegrasikan dalam setiap komponen KSP, seperti infografis berikut ini.

Panduan Integrasi Kurikulum Pendidikan Keamanan Siber dalam Satuan Kurikulum Pendidikan

Komponen KSP	Deskripsi
Analisis Karakteristik Satuan Pendidikan	Saat menganalisis, **identifikasi juga ancaman siber di lingkungan satuan pendidikan**, serta tentukan kompetensi pendidikan keamanan siber yang perlu dipelajari. **Sumber data**: pemetaan penggunaan teknologi di sekolah dan pemetaan risiko siber yang dilakukan bersama warga sekolah.
Visi, Misi, dan Tujuan Satuan Pendidikan	Dalam pengembangan visi, misi, dan tujuan, **nyatakan dengan jelas kompetensi pendidikan keamanan siber yang diharapkan berkembang pada diri murid (visi)**. Jelaskan **cara mencapainya** melalui berbagai kebijakan budaya keamanan siber yang akan diterapkan di satuan pendidikan **(misi)**.

Komponen KSP	Deskripsi
Pengorganisasian Pembelajaran	**Sisipkan materi dan keterampilan pendidikan keamanan siber dalam berbagai struktur kurikulum**, yang mencakup intrakurikuler, kokurikuler, ekstrakurikuler, serta pengembangan sikap dan pembiasaan (lihat Bab 4). Jika memungkinkan, **kembangkan kemitraan dengan lembaga yang kompeten** dalam bidang keamanan siber untuk mendukung pembelajaran ini (lihat Bab 5).
Perencanaan Pembelajaran	Pastikan proses pembelajaran **memperkenalkan isu keamanan siber yang dekat dengan keseharian murid**. Dorong mereka untuk mengeksplorasi berbagai pengetahuan tentang ancaman siber yang ada di sekitar mereka. Pastikan adanya **aksi nyata adaptasi dan mitigasi risiko siber** sebagai tindak lanjut, dan libatkan seluruh warga sekolah dalam aksi tersebut.

Dalam pengembangan Kurikulum Satuan Pendidikan (KSP) maupun kebijakan lainnya, seluruh warga sekolah perlu dilibatkan secara aktif. Partisipasi yang inklusif sangat penting, karena budaya keamanan siber tidak akan terwujud tanpa kesepakatan dan kerja sama dari semua pihak di sekolah.

Proses pengembangan KSP dimulai dengan analisis terhadap karakteristik satuan pendidikan, termasuk pemetaan tingkat kesadaran dan kesiapan keamanan siber di sekolah. Selanjutnya, pengembangan visi, misi, dan tujuan pendidikan keamanan siber dapat dilakukan secara partisipatif bersama seluruh warga sekolah, termasuk murid, pendidik, dan orang tua. Pada tahap perencanaan dan eksekusi, setiap warga sekolah dapat berperan aktif dalam mengisi aspek-aspek yang belum tercakup dalam pengorganisasian dan perencanaan pembelajaran.

Selain empat komponen utama KSP yang sudah dibahas di atas, sekolah juga direkomendasikan untuk melakukan evaluasi, pengembangan profesional, dan pendampingan sebagai bagian dari siklus peningkatan kualitas kurikulumnya. Evaluasi yang dilakukan secara mandiri dan berkala membantu sekolah meninjau capaian pembelajaran dan efektivitas strategi keamanan siber yang diterapkan, sementara hasilnya menjadi dasar bagi pengembangan profesional pendidik serta penguatan kompetensi terkait literasi digital dan perlindungan data. Pendampingan kemudian diberikan sebagai tindak lanjut untuk memastikan praktik pembelajaran dan kebijakan keamanan siber dijalankan secara konsisten dan responsif terhadap kebutuhan sekolah, sehingga seluruh warga sekolah dapat berkontribusi pada terbentuknya budaya keamanan siber yang kuat dan berkelanjutan.

Dengan pendekatan ini, budaya keamanan siber dapat terbentuk secara holistik dan menyeluruh, melalui partisipasi aktif dari semua elemen yang terlibat dalam kehidupan sekolah.

Bentuk Pelibatan Warga Sekolah

Komponen KSP	Bentuk Pelibatan
Analisis Karakteristik Satuan Pendidikan	Buat pertanyaan utama (***Define***) bersama seluruh warga sekolah, serta sepakati tujuan bersama dan hal-hal penting lainnya yang perlu diketahui bersama. Untuk membantu satuan pendidikan di dalam melakukan pemetaan, terlampir contoh rekomendasi lembar kerja untuk pemetaan terkait penggunaan teknologi dan budaya keamanan siber pada satuan pendidikan. Ambil pelajaran (***Discover***) - bersama warga sekolah, lakukan pemetaan dan penyelidikan untuk memahami karakteristik satuan pendidikan serta mengidentifikasi praktik baik yang telah dilakukan.
Visi, Misi, dan Tujuan Satuan Pendidikan	Gali mimpi (***Dream***) - kembangkan visi bersama tentang budaya keamanan siber di satuan pendidikan.
Pendidik: Pengorganisasian dan Perencanaan Pembelajaran	Jabarkan rencana (***Design***) - untuk mewujudkan visi tersebut, susunlah rencana aksi yang terukur hasilnya dan memiliki jangka waktu yang jelas.
Warga lain: Melengkapi dari aspek tata kelola, fasilitas-operasional, dan kemitraan komunitas	Atur eksekusi (***Deliver***) - laksanakan rencana yang telah disusun. Setiap warga sekolah dapat berperan sesuai tanggung jawab masing-masing dalam eksekusi. Lakukan evaluasi secara berkala dan lakukan penyesuaian berdasarkan temuan dari evaluasi tersebut.

Sumber: Cooperrider, D.L., Whitney, D., & Stavros, J.M. (2008) Appreciative Inquiry Handbook, Crown Custom Publishing, Inc.

"Halo! Saya Pak Rian, wakil kepala sekolah bidang kurikulum di SMP Nusantara. Mari simak bagaimana saya dan para guru mengintegrasikan pendidikan keamanan siber di SMP kami."

Langkah 1

Analisis Karakteristik Satuan Pendidikan

Dari rapor pendidikan, kami tahu bahwa SMP Nusantara masih perlu membenahi:

1. Kesadaran murid tentang keamanan data pribadi.
2. Penggunaan internet sehat dan bijak.
3. Kebiasaan warga sekolah dalam menjaga akun digital.

Pemetaan bersama warga sekolah menunjukkan bahwa murid sering menghadapi risiko siber seperti perundungan daring, akun diretas, dan penyebaran hoaks.

Langkah 2

Visi, Misi, dan Tujuan Satuan Pendidikan

Bersama warga sekolah, kami menyepakati visi SMP Nusantara yaitu:

"Sekolah aman siber, cerdas digital, dan bertanggung jawab."

Visi ini kami capai melalui:

1. Mengajarkan keterampilan dasar keamanan siber sejak dini.
2. Menyisipkan topik etika digital dan literasi informasi dalam pembelajaran.
3. Menyediakan program pendampingan untuk membentuk budaya aman siber.

Langkah 3

Pengorganisasian Pembelajaran

Penerapan visi-misi sekolah kami rancang dalam berbagai aspek pembelajaran.

- **Intrakurikuler**: materi keamanan siber disisipkan dalam pelajaran Informatika, Pendidikan Pancasila, dan Bahasa Indonesia (contoh: mengkritisi berita palsu).
- **Kokurikuler**: klub teknologi murid membuat poster digital tentang tips keamanan akun.
- **Ekstrakurikuler**: simulasi *cyber drill* untuk melatih respon jika akun diretas atau data bocor.
- **Budaya sekolah**: murid diajarkan untuk selalu *logout* setelah menggunakan perangkat bersama dan mengganti kata sandi secara berkala.

Langkah 4

Perencanaan Pembelajaran

Setelah pelatihan, para guru mulai punya banyak ide untuk merancang pembelajaran yang inovatif.

- Di mata pelajaran Informatika, Bu Rani mengajak murid membuat Jurnal Siber berisi catatan harian tentang aktivitas digital yang aman.
- Di mata pelajaran Pendidikan Pancasila, Pak Budi mengajak murid berdiskusi mengenai etika di dalam bermedia sosial.
- Di mata pelajaran Bahasa Indonesia, murid belajar menganalisis teks hoaks dan membandingkannya dengan sumber informasi tepercaya.

Dengan langkah-langkah ini, murid semakin sadar akan pentingnya melindungi informasi pribadi, berperilaku bijak di dunia maya, serta menjadi agen budaya aman siber di sekolah maupun di rumah.

Langkah 4

Evaluasi, Pengembangan Profesional, dan Pendampingan

Setelah program berjalan, kami melakukan evaluasi untuk memastikan integrasi pendidikan keamanan siber benar-benar efektif.

Evaluasi

- Mengumpulkan umpan balik melalui observasi kelas, jurnal murid, dan kuesioner.
- Menganalisis apakah murid lebih sadar akan keamanan data, etika digital, dan cara menangkal hoaks.
- Mencatat perubahan insiden siber sebagai indikator dampak program.

Pengembangan Profesional

- Guru mengikuti pelatihan lanjutan tentang literasi digital, hoaks, dan keamanan akun.
- Sesi berbagi praktik baik untuk memperkuat strategi mengajar topik keamanan siber.

Pendampingan dan Perbaikan

- Tim kurikulum mendampingi guru menyempurnakan perangkat ajar.
- Program pembelajaran disesuaikan berdasarkan hasil evaluasi.
- Melibatkan orang tua untuk penguatan budaya aman siber di rumah.

Dengan siklus evaluasi dan pendampingan yang berkelanjutan, sekolah kami terus memperkuat budaya aman siber bagi seluruh warga sekolah. Hasilnya, kesadaran murid meningkat, perilaku digital lebih aman, dan budaya “aman siber” mulai terbentuk di lingkungan SMP Nusantara.

Contoh Lembar Kerja
Pemetaan Budaya Keamanan Siber (1):

Identifikasi Risiko dan Kerentanan Keamanan Siber

Dilakukan bersama oleh warga sekolah. Beri tanda centang (✓) pada jawaban yang sesuai

 Apakah satuan pendidikan ...	 Jika ya, waspadai ...	 Respons yang dapat dipilih ...
Menggunakan perangkat digital (laptop, tablet, ponsel) dalam pembelajaran?	☐ Risiko pencurian data pribadi ☐ *Malware* dan *ransomware* ☐ Serangan *phishing*	☐ Pelatihan literasi digital dan keamanan siber ☐ Pemasangan antivirus dan *firewall* ☐ Kebijakan penggunaan perangkat pribadi
Menyimpan data digital (nilai, data murid, administrasi)?	☐ Kebocoran data sensitif ☐ Akses tidak sah ☐ Kehilangan data (*data loss*)	☐ Enkripsi data ☐ *Backup* data rutin ☐ *Access control* dan autentikasi multi-faktor
Memiliki jaringan WiFi yang dapat diakses oleh warga sekolah?	☐ Penyusupan jaringan ☐ Serangan *Man-in-the-Middle* ☐ Penggunaan *bandwidth* tidak wajar	☐ Segmentasi jaringan (tamu *versus* internal) ☐ Penggunaan VPN ☐ Monitoring lalu lintas jaringan
Menggunakan platform digital (*e-learning, cloud storage*, media sosial)?	☐ Akun diretas ☐ Penyalahgunaan akses ☐ Konten tidak pantas	☐ Pelatihan privasi dan keamanan akun ☐ Pengaturan privasi yang ketat ☐ Pelaporan insiden siber
Memiliki murid/pendidik yang aktif menggunakan media sosial?	☐ *Cyberbullying* ☐ Jejak digital negatif ☐ Penipuan online	☐ Edukasi digital *citizenship* ☐ Panduan etika bermedia sosial ☐ Mekanisme pelaporan

Contoh Lembar Kerja
Pemetaan Budaya Keamanan Siber (2):

Modal dan Sumber Daya untuk Membangun Budaya Keamanan Siber

Dilakukan bersama oleh warga sekolah. Beri tanda centang pada jawaban yang sesuai

Jenis Modal	Bentuknya dapat berupa ...	Cara mengoptimalkan ...
Modal Manusia	☐ Pemahaman dasar keamanan siber ☐ Tenaga IT atau guru TIK ☐ Relawan/orang tua dengan latar belakang IT ☐ Perilaku sadar siber yang sudah terbiasa	☐ Pelatihan rutin untuk pendidik dan murid ☐ Membentuk tim siber sekolah ☐ Mengundang ahli/ narasumber eksternal
Modal Sosial	☐ Forum diskusi tentang literasi digital ☐ Jejaring dengan komunitas siber atau kampus ☐ Kemitraan dengan penyedia layanan keamanan siber	☐ Membuat klub atau komunitas siber sekolah ☐ Kolaborasi dengan pihak eksternal untuk simulasi serangan siber
Modal Kebijakan	☐ Adanya kebijakan penggunaan teknologi (AUP) ☐ SOP penanganan insiden siber ☐ Regulasi pelindungan data pribadi	☐ Sosialisasi kebijakan ke seluruh warga sekolah ☐ Evaluasi dan update kebijakan secara berkala
Modal Teknologi	☐ *Software* keamanan (antivirus, *firewall)* ☐ Infrastruktur jaringan yang aman ☐ *Tools monitoring* dan *backup* data	☐ Pemeliharaan rutin perangkat dan *software* ☐ *Upgrade* sistem sesuai kebutuhan
Modal Finansial	☐ Dana BOS untuk pengembangan digital ☐ Bantuan dari komite sekolah atau CSR perusahaan	☐ Alokasi dana untuk pelatihan, *tools*, dan infrastruktur keamanan

Informasi Penting

Apakah Anda mengetahui bahwa, terlalu lama menatap layar bukan hanya membuat mata lelah, tapi juga dapat memengaruhi cara anak belajar, berinteraksi, dan merasakan emosi?

Penelitian menunjukkan bahwa dampak penggunaan perangkat digital tidak semata bergantung pada lamanya waktu di depan layar, tetapi juga pada jenis aktivitas, konten yang diakses, dan pengalaman digital yang dialami anak. UNICEF (2025) mencatat bahwa paparan pengalaman negatif di dunia maya, seperti perundungan atau pelecehan online, berisiko lebih besar menimbulkan kecemasan dan perilaku menyakiti diri dibandingkan durasi layar itu sendiri.

Karena itu, pembatasan screen time tetap penting untuk menjaga kesehatan fisik, tidur, dan interaksi sosial anak. Tujuannya bukan sekadar mengurangi waktu layar, tetapi mendorong penggunaan yang sehat, aman, dan bermakna. Keputusan mengenai durasi sebaiknya disesuaikan dengan konteks keluarga dan sekolah, didukung oleh kebijakan publik, literasi digital berkelanjutan, dan regulasi terhadap platform digital agar lebih bertanggung jawab melindungi anak.

Usia Anak	Rekomendasi Durasi Penggunaan Perangkat	Sumber Referensi
 **Di bawah 1 tahun**	Tidak direkomendasikan, kecuali untuk panggilan video dengan keluarga.	WHO, 2019; UNICEF, 2025
 **1-2 tahun**	Tidak lebih dari 1 jam per hari (lebih sedikit lebih baik)	WHO, 2019; AAP, 2021
 **2-5 tahun**	Maksimal 1 jam per hari, difokuskan pada konten berkualitas dan interaksi bersama orang tua/pengasuh.	WHO, 2019; AAP, 2021
 **5-10 tahun**	Maksimal 2 jam per hari, tanpa mengganggu tidur, aktivitas fisik, interaksi sosial, dan waktu belajar.	WHO, 2019; AAP, 2021
 **10-17 tahun**	Maksimal 2 jam per hari di luar tugas sekolah.	OSF Healthcare, 2024

BAB
4

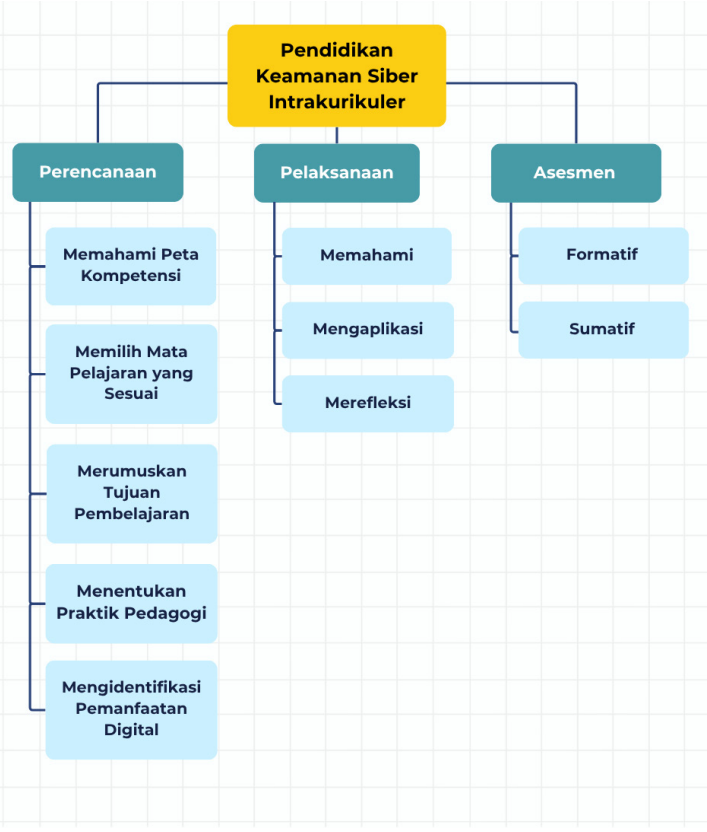
Implementasi Pendidikan Keamanan Siber dalam Pembelajaran

BAB 4

Implementasi Pendidikan Keamanan Siber dalam Pembelajaran

A Implementasi di Intrakurikuler

Intrakurikuler adalah kegiatan pembelajaran utama dan pokok yang dilaksanakan di sekolah sesuai dengan kurikulum satuan pendidikan yang telah dirumuskan. Pendidikan keamanan siber dapat dilaksanakan secara intrakurikuler dengan cara diintegrasikan ke dalam mata pelajaran wajib atau pilihan yang telah diprogramkan dalam kurikulum satuan pendidikan, meliputi tahap perencanaan, pelaksanaan, dan asesmen. Ketiga tahapan ini mengikuti pendekatan pembelajaran mendalam dengan prinsipnya: berkesadaran, bermakna, dan menggembirakan. Pada pelaksanaannya, integrasi pendidikan keamanan siber dapat dilaksanakan dengan banyak variasi praktis sesuai dengan sumber daya yang dimiliki sekolah.

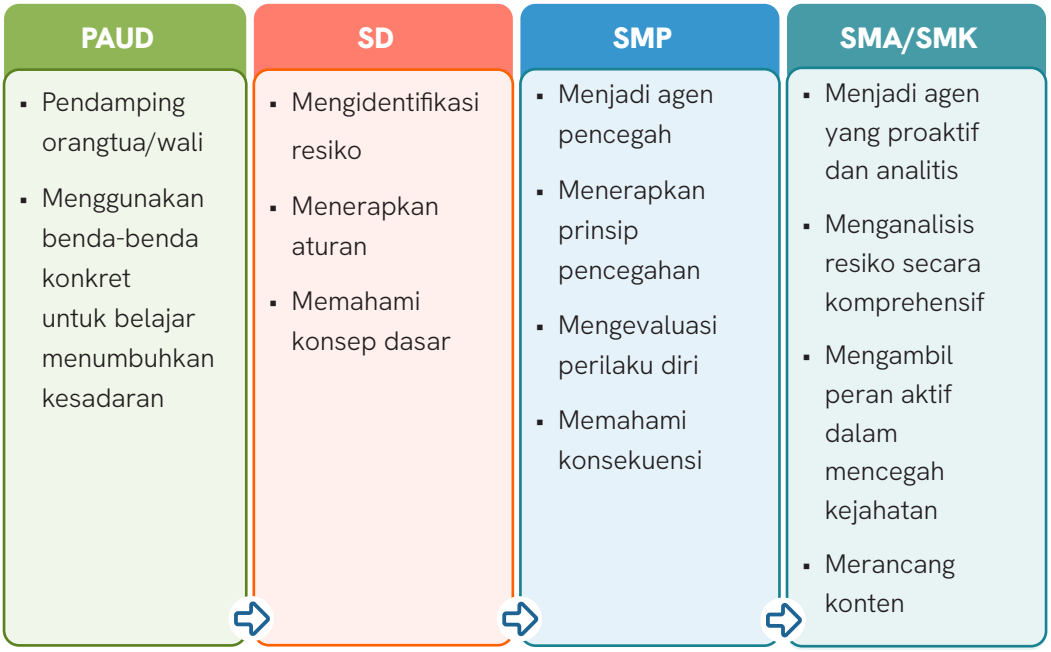


Gambar:
Implementasi Pendidikan Keamanan Siber Secara Intrakurikuler

4 Perencanaan dan Pelaksanaan Pembelajaran Kontekstualisasi Keamanan Siber

Memahami learning progression pada peta kompetensi pendidikan keamanan siber

Peta Kompetensi Keamanan Siber menyediakan kerangka kerja yang terstruktur untuk membangun kecakapan digital murid secara bertahap di seluruh jenjang pendidikan. Kerangka ini, sebagaimana yang telah dibahas pada Bab 2, terdiri dari lima elemen kompetensi utama dengan ***learning progression*** sebagai berikut:



Gambar: *Learning Progression* Pendidikan Keamanan Siber

Pada jenjang **PAUD**, anak diposisikan sebagai subjek yang perlu dilindungi, di mana hampir semua kompetensi menekankan pentingnya "pendampingan orang tua/wali atau pendidik". Di jenjang **SD**, murid mulai bertransisi menjadi agen yang sadar akan keamanan siber dengan batasan-batasan tertentu; mereka belajar "mengidentifikasi" risiko, "menerapkan aturan" yang ditetapkan, dan "memahami" konsep dasar seperti perbedaan informasi publik dan pribadi. Memasuki jenjang **SMP**, murid didorong untuk menjadi agen pencegahan. Kompetensi murid bergeser ke arah "menerapkan prinsip pencegahan," "mengevaluasi perilaku diri sendiri," dan memahami "konsekuensi" dari jejak digital. Puncaknya di jenjang **SMA/SMK**, murid diharapkan menjadi agen yang proaktif dan analitis. Mereka dituntut untuk mampu "menganalisis risiko" secara komprehensif, "mengambil peran aktif dalam mencegah" perundungan siber, dan "merancang" konten positif.

Implementasi setiap kompetensi pendidikan keamanan siber dapat dilaksanakan secara fleksibel pada fase atau tingkatan kelas, diawali dengan analisis kebutuhan murid. Apabila diperlukan, pendidik diperkenankan mengadaptasi kompetensi pendidikan keamanan siber dari jenjang sebelumnya untuk memastikan murid menguasai kompetensi yang dibutuhkan. Selain lintas fase, kompetensi pendidikan keamanan siber juga dapat diterapkan secara lintas elemen (menyelenggarakan satu pembelajaran dengan tujuan menguasai beberapa kompetensi dari elemen yang berbeda secara simultan), mengingat sejatinya setiap elemen pada pendidikan keamanan siber saling terkait dan tidak berdiri sendiri.

Perkembangan peran murid ini memiliki implikasi langsung terhadap pendekatan pedagogis yang harus diterapkan. Pembelajaran di PAUD dapat berfokus pada pembiasaan, pelindungan, dan interaksi yang dimediasi oleh orang dewasa. Sebaliknya, pembelajaran di SMA lebih mendorong agensi murid, pemikiran kritis, dan pengembangan tanggung jawab sosial melalui metode seperti debat, riset, dan proyek advokasi.

Mengintegrasikan Pendidikan Keamanan Siber ke Dalam Mata Pelajaran

Integrasi pembelajaran keamanan siber yang efektif bukanlah sekadar "menitipkan materi" tambahan yang membebani kurikulum. Sebaliknya, integrasi ini memanfaatkan isu-isu keamanan siber sebagai konteks yang otentik dan relevan untuk mencapai tujuan pembelajaran yang sudah ada di berbagai mata pelajaran. Pendekatan ini selaras dengan pendekatan Pembelajaran Mendalam, di mana murid dapat menerapkan pengetahuannya secara kontekstual.

Untuk menghasilkan integrasi yang optimal, pendidik dapat memulai dari menganalisis capaian pembelajaran pada mata pelajaran yang dipilih untuk merumuskan berbagai tujuan pembelajarannya. Dari tujuan pembelajaran tersebut, dapat dipilih yang sesuai untuk mengintegrasikan muatan pendidikan keamanan siber, dan bila perlu, tujuan pembelajaran dapat dirumuskan dengan mengakomodasi muatan pendidikan keamanan siber.

Gambar:
Inspirasi Tahapan Integrasi Muatan Pendidikan Keamanan Siber Ke Dalam Mata Pelajaran

Integrasi muatan pendidikan keamanan siber secara intrakurikuler harus bersifat fleksibel;

1. Dapat diintegrasikan di berbagai mata pelajaran sesuai dengan konteks kompetensi yang diajarkan dan sumber daya yang dimiliki sekolah.
2. Dapat diimplementasikan lintas fase/kelas atau lintas elemen

Ide integrasi jenjang PAUD

Aktivitas belajar di PAUD fokus pada **kegiatan fisik dan konkret**, memanfaatkan benda-benda yang dapat disentuh dan dilihat dengan mudah.

Elemen	Dasar-Dasar Literasi, Matematika, Sains, Teknologi, Rekayasa, dan Seni
Capaian pembelajaran	Murid menunjukkan kemampuan awal menggunakan dan merekayasa teknologi serta untuk mencari informasi, gagasan, dan keterampilan secara aman dan bertanggung jawab
Kompetensi pendidikan keamanan siber yang dipilih	Murid mengetahui perilaku aman saat menggunakan perangkat teknologi
c. Tujuan Pembelajaran yang Sesuai (👍🏻) dan Kurang Sesuai (🤔)	a. Murid memahami fungsi alat sederhana 🤔 b. Murid menggunakan alat sederhana untuk berbagai aktivitas 🤔 c. Murid memahami fungsi alat untuk memudahkan aktivitas dalam kehidupan sehari-hari 🤔 d. Murid menggunakan teknologi sederhana secara aman dan bertanggungjawab 👍
Ide integrasi	**Bermain peran:** mendemonstrasikan proses meminta izin kepada orangtua sebelum menggunakan gawai dengan bertanggungjawab

Ide integrasi jenjang SD

Di jenjang **SD**, murid mulai bertransisi menjadi agen yang sadar akan keamanan siber dengan batasan-batasan tertentu

Mata Pelajaran	Bahasa Indonesia
Elemen	Membaca dan Memirsa
Capaian Pembelajaran	Membaca kata-kata dengan berbagai pola kombinasi huruf dengan fasih dari bacaan dan/atau tayangan yang dipirsa; dan menganalisis informasi serta nilai-nilai dalam teks sastra dan nonsastra berwujud teks visual dan/atau audiovisual.
Kompetensi Pendidikan Keamanan Siber Yang Dipilih	Murid dapat mengidentifikasi ciri-ciri informasi yang meragukan
Tujuan Pembelajaran yang Sesuai (👍) dan Kurang Sesuai (🤔)	a. Membaca kata-kata dengan berbagai pola kombinasi huruf dengan fasih dari bacaan dan/atau tayangan yang dipirsa. 🤔 b. Menganalisis informasi dalam teks sastra berwujud teks visual dan/atau audiovisual 🤔 c. Menganalisis informasi nonsastra berwujud teks visual dan/atau audiovisual. 👍 d. Menganalisis nilai-nilai dalam teks nonsastra berwujud teks visual dan/atau audiovisual.👍
Ide Integrasi	**Galeri Informasi "Fakta atau Fiksi?"** Pendidik menyiapkan beberapa contoh cetakan teks singkat, tangkapan layar percakapan, atau gambar dan menempelkannya di dinding kelas seperti sebuah galeri seni. Murid, yang dibekali dengan catatan kecil atau stiker berwarna (misalnya, hijau untuk "Fakta", kuning untuk "Perlu Dicek", dan merah untuk "Fiksi"), diminta untuk berkeliling galeri. Mereka mengamati setiap informasi dan menempelkan stiker sesuai penilaian mereka, dan menuliskan/mengutarakan alasannya.

Ide integrasi jenjang SMP

Pendidikan keamanan siber pada jenjang SMP fokus pada kontekstualisasi pengetahuan dan pemantapan keterampilan untuk mengamankan diri di ruang siber.

Mata pelajaran	Bahasa Inggris
Elemen	**Menulis - Mempresentasikan *(Writing - Presenting)***
Capaian Pembelajaran	Murid mengomunikasikan gagasan dan pengalaman mereka dalam berbagai jenis teks secara tertulis atau teks multimodal tentang topik sehari-hari dan sesuai dengan minat dengan mulai menggunakan kalimat sederhana dan majemuk dengan struktur teks dan unsur kebahasaan yang tepat. Murid mengungkapkan pendapat dan mempertahankan argumen tentang suatu isu terkait topik sehari-hari atau yang sesuai dengan minat.
Kompetensi Pendidikan Keamanan Siber Yang Dipilih	Murid dapat menganalisis dampak jejak digital terhadap reputasi pribadi
Tujuan Pembelajaran yang Sesuai (👍) dan Kurang Sesuai (🤔)	▪ Mengungkapkan gagasan dalam berbagai jenis teks secara tertulis tentang topik sehari-hari dan sesuai dengan minat dengan mulai menggunakan kalimat sederhana dan majemuk dengan struktur teks dan unsur kebahasaan yang tepat.🤔 ▪ Mengomunikasikan gagasan dan pengalaman dalam teks multimodal tentang topik sehari-hari dan sesuai dengan minat dengan mulai menggunakan kalimat sederhana dan majemuk dengan struktur teks dan unsur kebahasaan yang tepat.🤔 ▪ Mengungkapkan pendapat tentang suatu isu terkait kehidupan sehari-hari dan yang sesuai dengan minat.👍 ▪ Mempertahankan pendapat tentang suatu isu terkait kehidupan sehari-hari dan yang sesuai dengan minat.👍
Ide Integrasi	**Studi kasus jejak digital:** murid mengkaji/menganalisis suatu kasus tentang jejak digital seorang tokoh media sosial (*influencer*) dan mempresentasikan hasilnya yang meliputi pendapatnya tentang dampak positif & negatif dari jejak digital terhadap reputasi *influencer* tersebut dan meluaskan konteksnya ke reputasi pribadi murid.

Ide integrasi jenjang SMA

Pada jenjang SMA murid diharapkan menjadi agen yang proaktif dan analitis, lebih mandiri, dan mampu merancang berbagai kegiatan atau konten untuk mengedukasi lingkungan sekitarnya.

Mata Pelajaran	Koding dan Kecerdasan Artifisial
Elemen	**Literasi Digital**
Capaian Pembelajaran	Pada akhir Fase E, murid mampu menerapkan produksi dan diseminasi konten digital dalam bentuk sajian multimedia.
Contoh Kompetensi Pendidikan Keamanan Siber Yang Dipilih	Murid dapat memproduksi dan menyebarkan konten perilaku positif.
Tujuan Pembelajaran yang Sesuai (👍) dan Kurang Sesuai (🤔)	▪ Memahami konsep dasar teknologi digital 🤔 ▪ Memahami keamanan informasi pribadi👍 ▪ Menerapkan internet secara aman dan produktif👍 ▪ Memahami dampak teknologi digital👍 ▪ Menerapkan produksi konten digital dalam bentuk teks dan gambar👍
Ide Integrasi	Memproduksi konten untuk kampanye “saling jaga”, bekerjasama dengan orang tua dan komunitas sekitar dengan tujuan mencegah perundungan di ruang siber.

Ide integrasi jenjang SMK

Pendidikan keamanan siber di jenjang SMK sebaiknya diintegrasikan dengan mempertimbangkan karakteristik unik setiap konsentrasi keahlian. Diharapkan pendidikan ini dapat mendukung kompetensi murid SMK dalam mempersiapkan diri untuk bekerja, berwirausaha, atau melanjutkan studi. Sebagai contoh, pendidikan keamanan siber dapat mendukung murid asisten keperawatan untuk memahami privasi pasien dan bertanggung jawab dalam mengelola keamanan data pasien, sedangkan di konsentrasi Teknik Komputer dan Jaringan (TKJ) atau kelompok SMK Teknologi Informasi, pendidikan keamanan siber dapat menjadi prasyarat penting sebelum mempelajari kompetensi keamanan siber tingkat lanjut, seperti evaluasi keamanan sistem, *ethical hacking*, atau *hashing*.

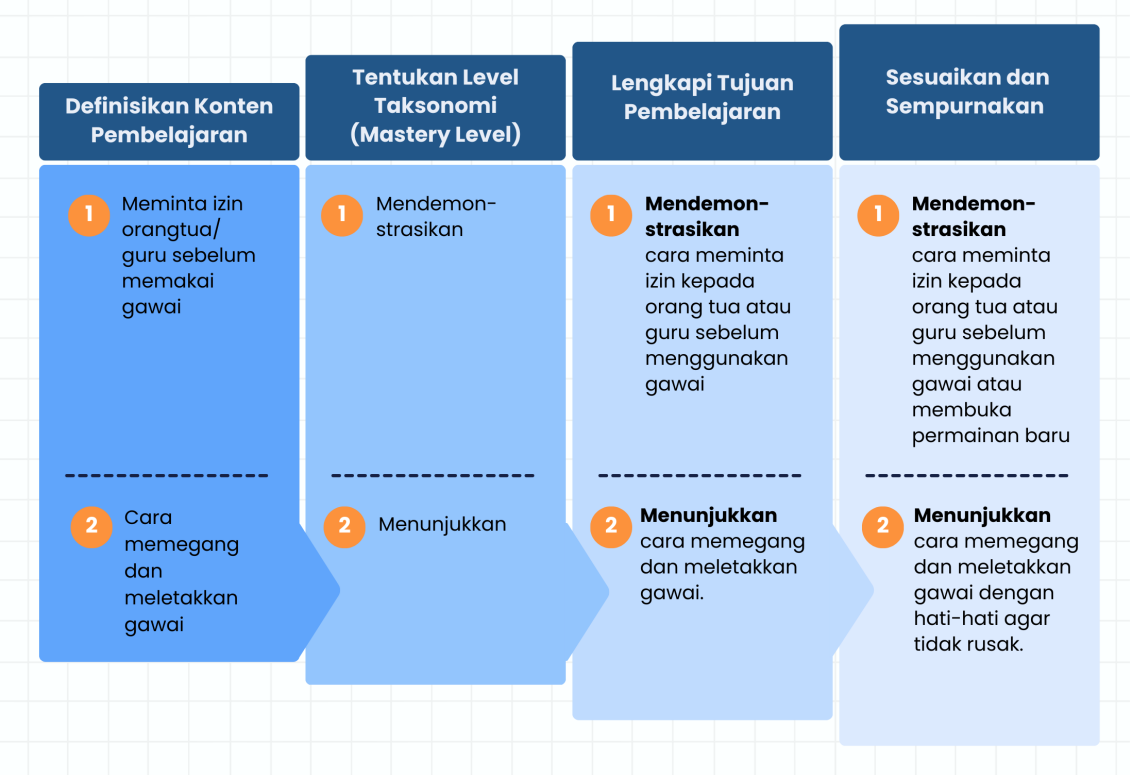
Berikut ini adalah contoh ide integrasi pada jenjang SMK di kelompok Kesehatan dan Pekerjaan Sosial:

Mata Pelajaran	Dasar-Dasar Pekerjaan Sosial (Fase E)
Elemen	Wawasan Dunia kerja Bidang Pekerjaan Sosial
Capaian Pembelajaran	Menganalisis aktivitas pekerjaan sosial termasuk penerimaan klien, identifikasi kebutuhan klien,perencanaan pemberian layanan, pelaksanaan pemberian layanan. evaluasi pemberian layanan, peluang usaha dan peluang kerja/profesi di bidang layanan pekerjaan sosial. murid juga memiliki kemampuan menganalisis perkembangan teknologi pada pekerjaan sosial mulai dari teknologi konvensional sampai kepada teknologi revolusi industri 4.0. serta Murid mampu mengidentifikasi perilaku filantropi dan *Job Profile*
Kompetensi Pendidikan Keamanan Siber Yang Dipilih	Murid dapat memahami prinsip manajemen identitas daring
Tujuan Pembelajaran yang Sesuai (👍) dan Kurang Sesuai (🤔)	▪ Menganalisis aktivitas pekerjaan sosial termasuk penerimaan klien, identifikasi kebutuhan klien, perencanaan pemberian layanan, pelaksanaan pemberian layanan. 🤔 ▪ Mengevaluasi pemberian layanan🤔 ▪ Menganalisis perkembangan teknologi pada pekerjaan sosial mulai dari teknologi konvensional sampai kepada teknologi revolusi industri 4.0. 👍 ▪ Mengidentifikasi perilaku filantropi dan *Job Profile*👍
Ide Integrasi	Perkenalkan aturan "**Uji 5 Detik Reputasi**": Sebelum memposting sesuatu di ruang siber, tanyakan pada diri sendiri 5 pertanyaan dalam 5 detik: 1. Apakah ini sesuatu yang **saya banggakan**? 2. Apakah ini akan **mempermalukan** saya di masa depan? 3. Apakah ini akan menyakiti **perasaan orang lain**? 4. Apakah saya nyaman jika **orang paling penting** dalam hidup saya (orang tua, pendidik, bos impian) melihatnya? 5. Apakah ini bersifat **permanen**? Setelah itu, murid mendiskusikan dampak jejak digital yang buruk terhadap berbagai profesi di bidang pekerjaan sosial.

Berbagai ide integrasi pendidikan keamanan siber lainnya dapat disimak **di bagian lampiran**

Merumuskan Tujuan Pembelajaran dan Kriteria Ketercapaian Tujuan Pembelajaran

Setelah peta kompetensi dan strategi integrasi dipahami, langkah berikutnya adalah menerjemahkannya ke dalam perencanaan pembelajaran operasional. Tahap ini dimulai dengan merumuskan Tujuan Pembelajaran (TP) dan Kriteria Ketercapaian Tujuan Pembelajaran (KKTP) yang terukur. Perumusan TP melibatkan penguraian kompetensi umum menjadi tujuan yang lebih spesifik. TP yang efektif mencakup **Kompetensi** (kemampuan yang ditunjukkan/didemonstrasikan melalui kata kerja operasional) dan **Lingkup Materi** (konteks keamanan siber).



Gambar: Menyusun Tujuan Pembelajaran. Diadaptasi dari https://cteresources.bc.edu/documentation/learning-objectives/

Tabel 5 Contoh Merumuskan Kriteria Ketercapaian Tujuan Pembelajaran

Kompetensi	*Murid mengetahui perilaku aman dan bertanggungjawab saat menggunakan perangkat teknologi dan berkomunikasi secara daring (PAUD)*
Contoh tujuan pembelajaran (TP)	**Murid menggunakan teknologi sederhana secara aman dan bertanggungjawab**
Contoh Kriteria ketercapaian	▪ Murid tidak memegang gawai sambil makan, minum, atau berlari-larian. ▪ Murid mampu meletakkan gawai dengan perlahan dan lembut ditempat yang aman dari risiko rusak ▪ Murid menggunakan permukaan yang datar, stabil, dan aman (seperti meja atau rak) untuk meletakkan gawai, bukan di lantai, di pinggir kursi, atau di tempat yang mudah terinjak.

Menentukan Praktik Pedagogi yang Sesuai

Menurut Nilson (2016), dalam menentukan model dan metode pembelajaran yang efektif, pendidik harus memulai dengan tujuan pembelajaran (*learning outcomes*) yang jelas. Pendekatan ini disebut sebagai desain pembelajaran yang berpusat pada hasil (*outcomes-centered course design*). Prosesnya dimulai dari pertanyaan mendasar: ***apa yang Anda ingin murid mampu lakukan di akhir pembelajaran?*** Setelah itu, barulah dipilih metode atau alat (*tools*) yang paling tepat untuk membantu murid mencapai tujuan tersebut.

Model Pembelajaran	***Metode Pembelajaran***
Sebuah kerangka yang lebih besar dan berorientasi pada hasil akhir pembelajaran. Model ini memberikan pendekatan dasar dalam mengajar, yang dapat berfokus pada pendidik atau murid	*Strategi dan teknik spesifik yang digunakan di dalam model pembelajaran untuk memfasilitasi interaksi dan aktivitas belajar*

Gambar: Model vs Metode Pembelajaran (Liu & Shi, 2007)

Dalam konteks pendidikan keamanan siber, praktik pedagogi yang sesuai dapat ditentukan utamanya melalui *mastery level* (tingkat kemahiran yang diharapkan) dan karakteristik murid. Misalnya, pada keterampilan teknis keamanan siber, *mastery level* yang diharapkan pada umumnya ialah menguasai **penerapan**. Maka, praktik pedagogi yang dapat digunakan adalah yang memungkinkan murid untuk mendapatkan pengalaman **belajar aktif dan mandiri**, misalnya **pembelajaran berbasis proyek menggunakan metode diskusi**.

Contoh penentuan praktik pedagogi pendidikan keamanan siber:

Tujuan pembelajaran:

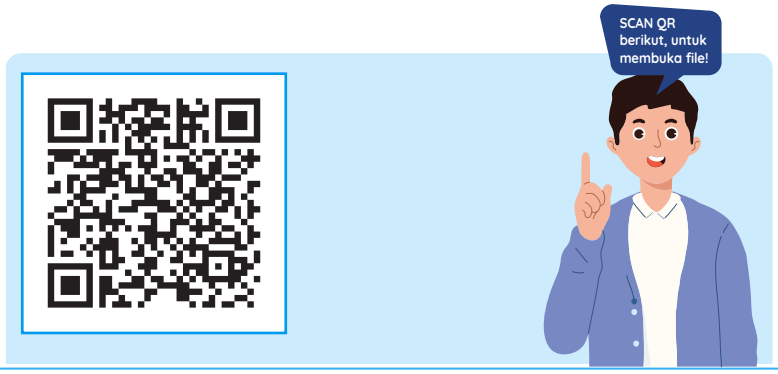
"Murid mampu **menerapkan** dan **mengevaluasi** berbagai strategi pengamanan perangkat dan akun yang dimiliki, untuk melindungi data pribadi dan identitas digitalnya."

Tujuan ini mencakup tingkat kognitif tinggi seperti **menerapkan** dan **mengevaluasi**. Metode dan model pembelajaran yang paling sesuai adalah yang berpusat pada murid.

Mengapa?

Karena **tujuan pembelajaran tersebut melibatkan tingkat kognitif tinggi yang sulit dicapai dengan menyimak atau mengikuti instruksi langsung.** Level "menerapkan" dan "mengevaluasi" menuntut keterlibatan aktif dan mandiri dari murid dalam proses belajar.

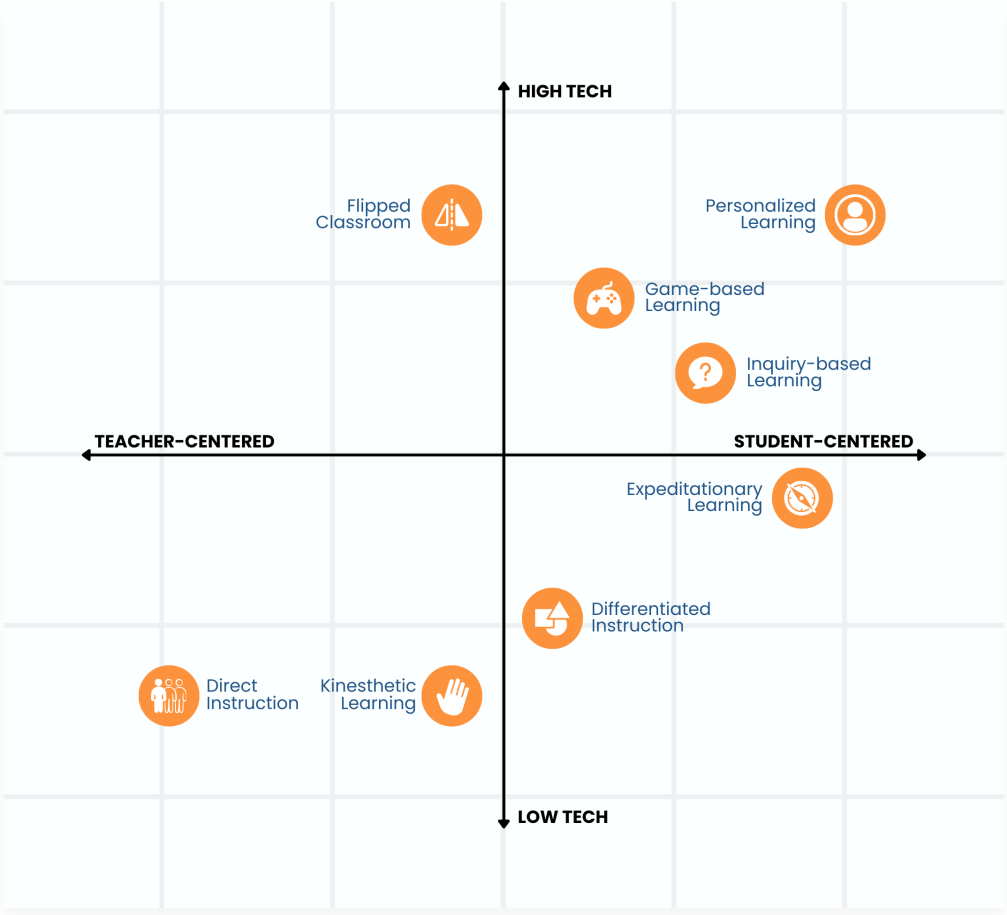
Detailnya dapat diamati pada *breakdown* **contoh kondisi** berikut ini:

Taksonomi tujuan pembelajaran (mastery level)	**Menerapkan, mengevaluasi**
Bahan ajar yang tersedia	**Modul SIBERKREASI Aman Digital** (*Digital Safety*) https://ringkas.kemendikdasmen.go.id/ModulAmanDigital 
Durasi waktu	**3 Pertemuan (@ 90 menit)**
Lingkungan belajar	**Ruang kelas fisik dan** *learning management system* **(LMS)**
Jumlah murid	**36**

Contoh Praktik Pedagogi yang Sesuai	***Problem-Based Learning* dengan metode diskusi kelompok dan simulasi atau *Case-Based Learning* dengan metode debat dan *role-play*** Alasan: ▪ Termasuk model pembelajaran berpusat pada murid untuk memberi pengalaman belajar yang aktif ▪ Durasi yang tersedia cukup untuk menyelesaikan kasus atau masalah sederhana, serta menyimulasikan penerapan strategi pelindungan akun dan data ▪ Jumlah murid mencukupi untuk pembagian kelompok kecil ▪ Terdapat ruang kelas dan LMS yang dapat digunakan sebagai sarana diskusi ▪ Bahan ajar bisa menjadi acuan untuk mengarahkan penggalian informasi yang dibutuhkan dalam penyelesaian kasus
Contoh Praktik Pedagogi yang Tidak Sesuai	**Instruksi langsung/*direct instruction*, ceramah, dan metode-metode berpusat pada pendidik lainnya (*teacher centered learning*).** Alasan: ▪ Kemampuan untuk menerapkan, menganalisis, dan mengevaluasi membutuhkan pengalaman belajar yang aktif ▪ Tujuan pembelajaran menuntut murid untuk menerapkan pengetahuannya secara langsung untuk kemudian mengevaluasinya

Mengidentifikasi Pemanfaatan Digital

Menentukan pemanfaatan digital yang tepat harus dimulai dengan mengidentifikasi tujuan dan praktik pedagogi yang ingin diterapkan. Kuadran berikut ini dapat berfungsi sebagai salah satu inspirasi untuk melihat posisi ideal praktik pedagogi yang digunakan.



Gambar: Kuadran Kebutuhan Teknologi dalam Pembelajaran.

Diadaptasi dari : https://teach.com/what/teachers-know/teaching-methods/

Langkah pertama adalah menentukan apakah pembelajaran akan **berpusat pada pendidik** atau **berpusat pada murid**.

	Karakteristik Utama	Kebutuhan Teknologi
Berpusat pada pendidik ***(Teacher-Centered)***	Pendidik sebagai penyampai informasi utama. Fokus pada penyampaian konten secara efisien.	Teknologi harus mendukung **transfer informasi** dan **manajemen kelas**.
Berpusat pada murid ***(Student-Centered)***	Murid sebagai agen aktif dalam pembelajaran. Fokus pada eksplorasi, penemuan, dan pembangunan pengetahuan.	Teknologi harus mendukung **kolaborasi, kustomisasi, penelitian,** dan **produksi konten** oleh murid.

Contoh: Jika pendidik memilih ***Direct Instruction*** (kuadran kiri bawah), teknologi yang dibutuhkan bisa jadi hanya berupa proyektor atau papan tulis interaktif sederhana. Jika pendidik memilih ***Personalized Learning*** (kuadran kanan atas), pendidik memerlukan platform *Learning Management System* (LMS) yang lebih kompleks dengan fitur yang adaptif (mampu beradaptasi dengan kemajuan belajar murid secara otomatis).

Langkah kedua adalah menentukan tingkat teknologi yang paling sesuai untuk mendukung metode yang dipilih di Langkah 1, apakah termasuk *High-Tech* atau *Low-tech*. Penentuan ini tidak dapat dilepaskan dari kondisi sarana dan prasarana serta sumber daya lain yang dimiliki sekolah.

Kuadran *LOW TECH*	Kuadran *HIGH TECH*
Mendukung aktivitas fisik, *hands-on*, atau penyampaian dasar. Teknologi harus minimal, terjangkau, dan sederhana.	Memungkinkan adanya dukungan terhadap kustomisasi, interaksi *real-time*, simulasi, dan akses ke berbagai sumber daya dari berbagai lokasi. Untuk kuadran ini, teknologi harus canggih dan terintegrasi

Setelah menetapkan posisi ideal dalam kuadran, pilih teknologi spesifik yang **memperkuat** keunggulan praktik pedagogi yang digunakan.

Tabel 6 Contoh Penentuan Kebutuhan Teknologi Spesifik Untuk Dijadikan Pemanfaatan Digital

Kuadran	Contoh Praktik Pedagogi	Fokus Pembelajaran	Kebutuhan Teknologi Spesifik
Kiri Bawah (*Low Tech, Teacher-Centered*)	*Direct Instruction*	Transmisi konten, Latihan *Drill & Practice.*	Proyektor, Perangkat lunak presentasi.
Kanan Bawah (*Low Tech, Student-Centered*)	*Differentiated Instruction, Expeditionary Learning*	Penemuan mandiri, Praktik, Aktivitas kelompok.	Aplikasi *productivity* sederhana (pengolah dokumen/*spreadsheet*), Kompas/GPS sederhana, Alat *sketching/mind-mapping*.

Kuadran	Contoh Praktik Pedagogi	Fokus Pembelajaran	Kebutuhan Teknologi Spesifik
Kiri Atas (*High Tech, Teacher-Centered*)	*Flipped Classroom*	Gabungan aktivitas di luar kelas dan dalam kelas, misal: persiapan konten di luar kelas, dilanjutkan aktivitas di dalam kelas.	Platform Video *Hosting* (YouTube/Vimeo), Alat perekam layar, LMS untuk distribusi konten.
Kanan Atas (*High Tech, Student-Centered*)	*Personalized Learning, Game-based Learning*	Kustomisasi alur belajar, Umpan balik segera, Eksplorasi mendalam.	Platform Pembelajaran Adaptif, Simulasi interaktif, Alat Gamifikasi, Perangkat lunak Kolaborasi.

Setelah dilakukan pemilihan pemanfaatan digital, lakukan langkah evaluasi:

1. **Ketersediaan & Akses:** Pastikan teknologi mudah diakses oleh pendidik dan murid (koneksi internet, perangkat).
2. **Penguasaan pendidik:** Sediakan waktu yang memadai agar pendidik dapat menggunakan teknologi secara efektif untuk mendukung pembelajaran (bukan hanya sebagai alat tambahan).
3. **Uji Coba:** Lakukan uji coba berskala kecil dan kumpulkan umpan balik tentang bagaimana teknologi benar-benar meningkatkan hasil belajar.

Contoh mengidentifikasi pemanfaatan digital pada pendidikan keamanan siber:

Tujuan pembelajaran:

*Murid mampu **mengevaluasi** informasi digital berdasarkan kriteria akurasi, kebenaran faktual, relevansi terhadap kebutuhan, kejelasan, kelengkapan, kreatifitas, etika, dan potensi bias.*

1. Analisis Kebutuhan Pedagogis (Sumbu X)

Tujuan ini mengharuskan murid untuk **mengevaluasi** informasi secara mandiri atau berkelompok, sehingga dibutuhkan eksplorasi informasi digital yang komprehensif.

Praktik Pedagogi yang Disarankan	**Berpusat pada murid:** ***Inquiry-based Learning*** atau ***Expeditionary Learning***: murid harus menanggapi tantangan, misalnya menganalisis berita viral, memverifikasi klaim di media sosial, atau membedah suatu sumber informasi.

2. Penentuan Tingkat Teknologi yang Diperlukan (Sumbu Y)

Karena objek pembelajaran adalah **informasi digital**, interaksi murid harus terjadi dalam lingkungan digital yang otentik (bukan hanya simulasi). Menggunakan teknologi tingkat rendah (misalnya hanya menggunakan presentasi ***slides***) kurang memadai untuk mengajarkan keterampilan melakukan verifikasi.

Tingkat Teknologi	***High Tech***: murid memerlukan akses ke **perangkat digital** yang dapat digunakan untuk mengakses, memverifikasi silang, dan menganalisis sumber informasi daring.
Fungsi Teknologi	**Simulasi & Verifikasi**: Teknologi harus mampu mereplikasi situasi dunia nyata (berinteraksi dengan hoax, mengecek metadata, mencari sumber terbalik/*reversed search*).

3. Pemilihan Teknologi Berdasarkan Kuadran (Integrasi)

Dengan posisi ideal di kuadran **Kanan Atas** (*High Tech, Student-Centered*), teknologi yang dipilih harus mendukung eksplorasi secara mendalam dan analisis kritis.

Teknologi	Peran dalam Pembelajaran
Mesin Pencari Lanjutan (Google Advanced Search), Google Scholar, Database Jurnal (misalnya DOAJ, ResearchGate)	Mengajarkan murid cara menyaring hasil pencarian, menemukan sumber primer, dan membandingkan sumber populer vs. sumber ilmiah.

Teknologi	Peran dalam Pembelajaran
Alat Pemeriksa Fakta (misalnya Snopes, Turnitin, cekfakta.com), Reverse Image Search (Google Lens, TinEye), Metadata Viewer	Memungkinkan murid untuk memverifikasi klaim, melacak asal-usul gambar atau video, dan mengidentifikasi bias atau klaim palsu dalam sumber.
Platform LMS (Google Classroom/ Moodle), Google Docs/Slides, Alat Presentasi Interaktif (Nearpod, Mentimeter)	Digunakan untuk mengelola tugas, membandingkan analisis kredibilitas, dan menyajikan hasil temuan verifikasi kepada kelas.
Platform Game/Simulasi Literasi Media	Menyediakan lingkungan aman dan menarik bagi murid untuk mempraktikkan keterampilan mendeteksi hoaks dan memahami mekanisme penyebaran disinformasi.

Menguraikan Langkah-Langkah Pembelajaran Dalam Pendekatan Pembelajaran Mendalam

Penerapan pembelajaran keamanan siber dalam kerangka pembelajaran mendalam dapat dilakukan dengan mengintegrasikan prinsip-prinsip pembelajaran mendalam ke dalam pengalaman belajar murid, yang meliputi tahapan **Memahami**, **Mengaplikasi**, dan **Merefleksi**. Terdapat tiga prinsip utama yang harus diterapkan, yang dapat diterapkan baik secara terpisah atau simultan:

- Berkesadaran (*Mindful*): Fokus, konsentrasi, dan perhatian murid diarahkan pada proses belajar. **Dalam konteks keamanan siber, ini bisa berarti murid sadar akan risiko siber dan ancaman yang ada di dunia digital.**
- Bermakna (*Meaningful*): Pembelajaran terhubung dengan kehidupan nyata dan relevan bagi murid, serta dapat diterapkan dalam berbagai konteks. **Contohnya, materi tentang jejak digital dikaitkan dengan dampak nyata pada reputasi pribadi murid.**
- Menggembirakan (*Joyful*): Menciptakan lingkungan belajar yang interaktif, menarik, dan memotivasi. **Pembelajaran keamanan siber dapat dirancang melalui tantangan atau aktivitas yang memotivasi murid untuk mencapai keberhasilan (Aha! moment).**

Contoh Kegiatan:

Memahami (Berkesadaran)

- Pendidik menampilkan contoh *e-mail phishing* (surel palsu yang tampak dari bank terkenal). Tantangan: Murid diminta mengidentifikasi tanda-tanda *phishing* dalam contoh tersebut (alamat pengirim yang aneh, tautan mencurigakan, terdengar sangat mendesak, dan sebagainya) dalam kelompok kecil. Perwakilan dari beberapa kelompok berbagi jawabannya.
- Murid menyimak video pendek (2-3 menit) tentang *malware* atau virus komputer yang menunjukkan bagaimana *malware* dapat masuk (contoh: mengunduh lampiran email tak dikenal). Murid diminta menyebutkan tindakan pencegahan malware (tidak sembarang klik link, memakai antivirus, *update* OS, dsb). Pendidik menuliskan poin-poin penting dari jawaban murid, menambah jika ada yang kurang (misal: jangan gunakan *software* bajakan karena rawan *malware*).

Mengaplikasi (Bermakna dan Menggembirakan)

- Murid mengaktifkan dan mengkonfigurasi verifikasi dua langkah untuk mengamankan akun perpesanan digital miliknya dan melakukan pengujian hasil aktivasi berdasarkan skenario yang telah disiapkan. Hasil pengujian didiskusikan bersama teman dalam kelompok kecil.
- Murid memeriksa kembali kata sandi pada akun gim daring yang mereka miliki dan menganalisis kekuatan kata sandinya sesuai kriteria panjang karakter, kombinasi huruf-angka-karakter khusus, dan penggunaan manajer kata sandi. Murid lalu memperbaiki kata sandinya jika hasil analisis menunjukkan bahwa kata sandi mereka lemah.
- Murid secara kelompok mensimulasikan menjadi "Tim Ahli Keamanan Siber" yang bertugas membuat panduan keamanan siber sederhana untuk sebuah organisasi (misal: satuan pendidikan sendiri atau perusahaan fiktif tempat magang). Panduan tersebut mencakup aturan untuk melindungi privasi data, langkah menghadapi insiden (misal: kebocoran data), dan penggunaan teknologi keamanan tertentu

Merefleksi (Bermakna)

- Murid memanfaatkan VPN secara mandiri untuk melindungi anonimitasnya di dunia maya ketika memanfaatkan koneksi internet untuk melakukan berbagai kegiatan sehari-hari, utamanya pada saat berada di ruang publik.
- Murid mengomunikasikan manfaat, kelebihan, dan kekurangan dari VPN yang ia pakai kepada orang lain dan merefleksikan pada dirinya sendiri apakah teknik penggunaan dan konfigurasi VPN yang ia gunakan sudah efektif dalam melindungi anonimitas dirinya di ruang siber.

Dalam pelaksanaan pendidikan keamanan siber, pendidik dapat berperan sebagai:

- **Pencipta Kondisi**: pendidik berperan sebagai fasilitator yang menciptakan suasana kelas yang kondusif dan iklim pembelajaran yang positif.
- **Pemberi Dukungan** (*scaffolding*): Sediakan dukungan yang diperlukan, seperti peta konsep, alat bantu, atau penjelasan tambahan, untuk membantu murid menguasai materi.
- **Pendorong Kemandirian**: Dorong murid untuk mengambil inisiatif dan mengembangkan kepercayaan diri serta kemandirian mereka dalam belajar.

5 Asesmen Pembelajaran Kontekstualisasi Keamanan Siber

Asesmen dalam paradigma pembelajaran mendalam menekankan pentingnya umpan balik dan asesmen otentik. Asesmen tidak hanya berfungsi sebagai pengukuran ***(Assessment of Learning)*** tetapi juga sebagai alat perbaikan ***(Assessment for Learning)*** dan refleksi diri ***(Assessment as Learning)***. Ketiga asesmen tersebut berfungsi sebagai:

1. **Asesmen sebagai Pembelajaran (*Assessment as Learning*):** Berfungsi sebagai asesmen formatif yang memacu refleksi diri murid terhadap proses belajar mereka. Contoh instrumennya meliputi jurnal reflektif, penilaian diri (*self-assessment*), dan penilaian antar teman (*peer assessment*). murid didorong untuk mengambil tanggung jawab atas pembelajaran mereka sendiri.
2. **Asesmen untuk Pembelajaran (*Assessment for Learning*):** Berfungsi sebagai umpan balik bagi pendidik untuk menyesuaikan dan memperbaiki proses pembelajaran. Alat seperti peta konsep, umpan balik formatif, dan observasi digunakan untuk membantu murid memahami progres mereka, sekaligus membantu pendidik merefleksikan pembelajaran.
3. **Asesmen dalam Pembelajaran (*Assessment of Learning*):** Berfungsi sebagai asesmen sumatif yang bertujuan mengukur capaian akhir pembelajaran. Instrumen yang digunakan adalah tes lisan/tertulis, penilaian proyek, atau portofolio. Hasil asesmen ini juga digunakan sebagai umpan balik strategis untuk perbaikan rancangan pembelajaran di masa mendatang.

Kriteria ketercapaian tujuan pembelajaran (KKTP) adalah **salah satu tolok ukur** yang mendefinisikan tingkat penguasaan kompetensi yang diharapkan. Penentuan KKTP yang akurat (misalnya: melalui rubrik atau panduan penilaian) sangat penting untuk memberikan transparansi dan objektivitas kepada murid tentang apa yang diharapkan akan tercapai pada pembelajaran.

Contoh: Jika tujuan pembelajarannya adalah "***Murid mampu menjelaskan bentuk dan dampak perundungan siber***", salah satu KKTP yang terukur adalah: "***murid dapat mengidentifikasi minimal tiga bentuk perundungan daring dan menjelaskan minimal dua dampak sosial yang ditimbulkan dari tindakan tersebut, serta merumuskan tiga langkah pelindungan diri (blokir, lapor, atur privasi)"***. KKTP tersebut lalu dikembangkan menjadi instrumen penilaian.

Asesmen Formatif

Asesmen formatif yang dilaksanakan sebelum proses pembelajaran (asesmen awal pembelajaran) untuk mengukur pemahaman awal dan kebutuhan belajar murid sangat penting karena latar belakang pengetahuan digital dan paparan risiko siber setiap murid berbeda. Asesmen awal pembelajaran difokuskan pada pengukuran Kesadaran Keamanan Siber dan Etika Digital yang telah dimiliki murid sebelum materi diajarkan. Hasil dari asesmen ini digunakan untuk menyesuaikan strategi pembelajaran dan materi, memastikan pembelajaran menjadi relevan dan bermakna. Sedangkan asesmen formatif yang dilaksanakan selama proses pembelajaran, atau seringkali disebut sebagai asesmen proses, dapat menjadi masukan bagi pendidik untuk menentukan intervensi yang diperlukan sehingga tujuan pembelajaran tercapai.

Berikut ini contoh penggunaan asesmen formatif dalam konteks pendidikan keamanan siber:

1. **Remedial dan Intervensi Dini:** Jika analisis data formatif menunjukkan kelemahan pada suatu area (misalnya, kesulitan membedakan opini, fakta, dan propaganda), pendidik harus segera melakukan intervensi atau penyesuaian kegiatan belajar di kelas. Intervensi harus spesifik dan berfokus pada keterampilan yang belum tercapai, bukan sekadar pengulangan materi.
2. **Pengayaan:** Untuk murid yang secara konsisten menunjukkan penguasaan yang cepat, pendidik dapat memberikan tugas pengayaan, misalnya kegiatan yang menuntut analisis risiko siber lebih mendalam atau peran aktif, seperti meminta murid SMA untuk menyusun usulan kepada organisasi intra sekolah dalam rangka upaya pencegahan perundungan siber di sekolah.
3. **Refleksi pendidik:** Hasil asesmen formatif harus mendorong pendidik untuk merefleksikan dan merevisi rancangan/pelaksanaan pembelajaran mereka, memastikan kesesuaian dengan karakteristik murid dan efektivitas metodologi pengajaran.

Contoh desain asesmen formatif dapat disimak di Lampiran 3

Asesmen Sumatif

Penggunaan asesmen sumatif dalam konteks pendidikan keamanan siber memiliki dua fungsi utama: **Pengukuran Pencapaian Kompetensi Akhir** dan **Umpan Balik Pada Keseluruhan Program Pembelajaran**. Pengukuran pencapaian kompetensi akhir adalah mengukur secara formal sejauh mana murid telah mencapai hasil belajar dan kompetensi yang ditetapkan.

Contoh Penerapan Asesmen Sumatif Berdasarkan Elemen Pendidikan Keamanan Siber:

- **Pengukuran Keterampilan Teknis:** Asesmen sumatif menguji kemampuan murid untuk secara mandiri menerapkan langkah-langkah pengamanan yang kompleks, seperti menerapkan autentikasi dua faktor, manajemen sandi yang kuat, atau bahkan teknik kriptografi tertentu (untuk jenjang SMA). Karena sifatnya yang aplikatif, asesmen ini sering berbentuk *Penilaian Kinerja*.
- **Pengujian Kemampuan Analisis Risiko:** Asesmen akhir mengukur kemampuan murid untuk menganalisis risiko pada studi kasus yang kompleks, seperti mengevaluasi risiko pembuatan akun pada platform baru berdasarkan variabel tertentu (syarat dan ketentuan, hak akses, data yang diminta). Kegiatan ini memerlukan kemampuan berpikir tingkat tinggi (HOTS) yang idealnya diukur melalui analisis studi kasus.
- **Kesadaran Hukum dan Etika:** Pada elemen ini, asesmen sumatif digunakan untuk mengkonfirmasi bahwa murid tidak hanya menghafal berbagai aturan/hukum/kode etik, tetapi mampu menganalisis pelanggaran aturan di dunia siber (misalnya, membedakan pelanggaran ringan dan berat).

Selain sebagai alat ukur, hasil asesmen sumatif juga berfungsi sebagai refleksi penting bagi pendidik dan institusi. Contoh**:**

1. **Refleksi Pembelajaran pendidik:** Hasil asesmen sumatif digunakan pendidik untuk mengevaluasi efektivitas pembelajaran yang telah berlalu. Jika mayoritas murid gagal mencapai tujuan pembelajaran pada elemen tertentu (misalnya, kesulitan membedakan fakta dan propaganda), maka ini mengindikasikan bahwa metode pengajaran, media, alokasi waktu, atau sumber daya lainnya untuk materi tersebut perlu direvisi pada semester berikutnya.
2. **Perbaikan Rencana Pembelajaran Berikutnya:** Data asesmen sumatif menjadi *input* penting untuk merencanakan kegiatan pembelajaran selanjutnya, misalnya membantu mengidentifikasi area yang perlu penguatan atau intervensi yang lebih sesuai di masa depan.

3. **Audit Kurikulum:** Jika hasil sumatif di seluruh angkatan menunjukkan kelemahan kolektif yang signifikan pada elemen kompetensi tertentu (misalnya, Kesadaran Hukum), maka hal tersebut mengindikasikan perlunya audit kurikulum untuk memastikan materi yang diajarkan selaras dengan tuntutan kompetensi yang diharapkan.

Contoh desain asesmen sumatif dapat disimak di Lampiran 3

B Implementasi Pendidikan Keamanan Siber Pada Kokurikuler

Penyusunan program kokurikuler keamanan siber melibatkan beberapa tahapan kerja yang sistematis dan kolaboratif. Tujuannya adalah memastikan program yang dirancang relevan, bermakna, dan dapat diimplementasikan secara efektif

1. Pembentukan Tim Kerja Kokurikuler

   Satuan pendidikan harus membentuk tim kerja kokurikuler yang terdiri dari kepala sekolah, koordinator kokurikuler (atau pendidik yang ditugaskan sebagai koordinator pembelajaran berbasis proyek), pendidik kelas/mata pelajaran, tenaga kependidikan, dan pihak lain yang relevan. Tim ini bertanggung jawab atas seluruh proses, mulai dari perencanaan hingga evaluasi.

2. Analisis Satuan Pendidikan

   Tim kerja melakukan analisis untuk memetakan kebutuhan belajar murid dan sumber daya yang tersedia di sekolah. Hal ini meliputi:

   - Mengidentifikasi dimensi profil lulusan yang perlu diperkuat, seperti **penalaran kritis** untuk menyaring informasi dan **komunikasi** untuk berinteraksi secara etis.
   - Menilai minat dan bakat murid serta capaian pembelajaran intrakurikuler yang dapat diperdalam melalui kokurikuler.
   - Memetakan sumber daya yang dimiliki, termasuk sumber daya fisik (laboratorium komputer), manusia (pendidik Informatika atau praktisi keamanan siber), dan lingkungan (bekerja sama dengan lembaga terkait).

3. Merancang Program

Berdasarkan hasil analisis, tim kerja merancang program kokurikuler dengan langkah-langkah berikut:

- **Menentukan Dimensi Profil Lulusan**: Pilih dimensi yang akan menjadi fokus utama, seperti kemandirian, komunikasi, kreativitas, atau dimensi lainnya. Misalnya, jika analisis menunjukkan murid sering menggunakan fitur perpesanan dalam gim daring, maka dimensi komunikasi dapat dijadikan prioritas untuk menguatkan berkomunikasi empatik di ruang siber.
- **Memilih Tema Kegiatan**: Tema sebaiknya relevan dengan konteks sosial budaya dan karakteristik murid. Contohnya tema "Generasi Bijak Digital" atau "Wirausaha Lokal Berbasis Budaya".
- **Menetapkan Bentuk Kegiatan**: Pilih salah satu dari tiga bentuk kokurikuler yang disarankan:
  - **Pembelajaran kolaboratif lintas disiplin ilmu**: Mengintegrasikan lebih dari satu mata pelajaran untuk membahas tema keamanan siber.
  - **Gerakan 7 Kebiasaan Anak Indonesia Hebat (G7KAIH)**: Fokus pada pembentukan kebiasaan positif, seperti "Gemar Belajar" untuk meningkatkan literasi digital.
  - **Cara lainnya**: Mengembangkan kegiatan yang unik sesuai dengan nilai atau keunggulan sekolah, seperti mengadakan pagelaran seni dengan tema keamanan siber.
- **Merumuskan Tujuan Pembelajaran**: Rancang tujuan yang menggabungkan kompetensi (dimensi profil lulusan) dan konten (tema).
- **Menyesuaikan Alokasi Waktu**: Sesuaikan alokasi waktu tahunan dengan ketentuan yang berlaku. Satuan pendidikan dapat membagi waktu tersebut menjadi dua semester dan menyesuaikan alokasi untuk setiap kegiatan.
- **Merancang Aktivitas dan Asesmen**: Rancang kegiatan yang mendorong murid untuk memahami, mengaplikasi, dan merefleksikan materi. Sertakan asesmen formatif (selama proses) dan sumatif (di akhir kegiatan) untuk mengukur pencapaian dimensi profil lulusan (khusus untuk bentuk kokurikuler pembelajaran kolaboratif lintas disiplin ilmu, perlu juga mengukur pencapaian tujuan pembelajaran). Asesmen ini dapat berupa observasi, proyek, atau presentasi.

Ide program kokurikuler Jenjang PAUD

Dimensi Profil Lulusan	Topik Utama	Deskripsi
Kemandirian	**Kotak Rahasia**	▪ Ajak anak membuat dan menghias sebuah kotak (bisa dari kardus bekas). Jelaskan bahwa kotak ini adalah tempat untuk menyimpan benda-benda paling pribadi dan aman mereka, yang ***hanya*** boleh dibuka oleh mereka atau bersama orang tua/pendidik. ▪ Ajak anak untuk membuat kata sandi sederhana yang harus diucapkan/dituliskan untuk membuka kotak tersebut. ▪ Pendidik menggunakan alokasi jam kokurikuler untuk proyek membuat kotak rahasia dan setiap minggunya memberikan berbagai macam benda/souvenir kepada murid untuk disimpan di dalam kotak rahasia. Pastikan anak mengucapkan/menuliskan kata sandinya sebelum memasukkan benda ke dalam kotak. ▪ Di akhir semester, anak membawa pulang kotak rahasia tersebut, dan membukanya bersama orangtua / wali murid.

Ide Program Kokurikuler Jenjang SD

Dimensi Profil Lulusan	Topik Utama	Deskripsi
Kreativitas	**Jurnal aplikasi**	Murid (bersama orangtua) membuat jurnal mingguan aplikasi yang terpasang dan digunakan di rumah, baik di gawai maupun di komputer. Jurnal berisi: ▪ Nama aplikasi ▪ Batasan usia yang diatur oleh aplikasi ▪ Rata-rata durasi penggunaan aplikasi ▪ Pengalaman saat menggunakan aplikasi Selama alokasi jam kokurikuler (rutin tiap minggu), murid bersama pendidik merefleksikan jurnal tersebut dan mendiskusikan perilaku yang sudah sehat dan lebih sehat dalam berinteraksi di ruang siber.

Ide Program Kokurikuler Jenjang SMP

Dimensi Profil Lulusan	Topik Utama	Deskripsi
Komunikasi	**Kampanye "Mabar Aman"**	Selama alokasi jam kokurikuler, murid menyusun rencana dan memproduksi konten kampanye yang bertujuan untuk mensosialisasikan "mabar" (main bareng) yang aman dan nyaman, misalnya dengan tidak mengirimkan pesan-pesan negatif melalui fitur percakapan dalam platform gim daring saat "mabar".

Ide Program Kokurikuler Jenjang SMA/SMK

Dimensi Profil Lulusan	Topik Utama	Deskripsi
Penalaran Kritis	**Bedah Buku**	Selama alokasi jam kokurikuler, murid secara berkelompok menyusun rencana bedah buku tentang keamanan siber dan membaca buku-buku yang teridentifikasi untuk memutuskan buku yang akan dibedah di akhir semester. Setiap kelompok mempresentasikan poin-poin penting dari buku tersebut dan pendapatnya terhadap konten, kelebihan, dan kekurangan buku. Kelompok lainnya dapat bertindak sebagai pembanding atau panelis, dan mendiskusikan hasil bedah buku yang dipaparkan.

Dimensi Profil Lulusan	Topik Utama	Deskripsi
Kesehatan	**Ruang Ekspresi dan Relaksasi (*Mindfulness & Creative Space*)**	Menyediakan ruang fisik atau kegiatan rutin di sekolah yang mendorong murid untuk beristirahat, bersantai, dan mengekspresikan diri dengan cara yang sehat. murid dilibatkan dalam mendesain dan menata ulang sudut ruangan sekolah (misalnya di perpustakaan atau ruang OSIS) menjadi **Zona Nyaman** atau ruang relaksasi yang tenang (dengan musik lembut, tanaman, atau bantal). pendidik menggunakan waktu kokurikuler di zona nyaman untuk mendiskusikan hal-hal terkait reputasi diri, memitigasi kemungkinan terjadinya serangan siber yang mengganggu kondisi psikis atau fisik murid, dan memberi ruang aman agar murid berani melaporkan serangan yang terjadi.

C Implementasi Pendidikan Keamanan Siber Pada Ekstrakurikuler

Kegiatan ekstrakurikuler adalah kegiatan pengembangan karakter dalam rangka perluasan potensi, bakat, minat, kemampuan, kepribadian, kerja sama, dan kemandirian murid secara optimal yang dilakukan dengan bimbingan dan pengawasan satuan pendidikan. Jenis-jenis kegiatan ekstrakurikuler yang diatur dalam peraturan ini mencakup berbagai aktivitas yang dirancang untuk mendukung perkembangan holistik murid.

Program ekstrakurikuler dikembangkan dengan dua landasan utama. Pertama, kegiatan ini menyediakan wadah bagi murid untuk mengeksplorasi potensi dan kemampuan mereka, yang pada gilirannya mendukung kegiatan belajar mengajar secara keseluruhan. Kedua, ekstrakurikuler berfokus pada pengembangan kreativitas berdasarkan bakat dan minat yang telah dimiliki murid sejak dini. Selain itu, ekstrakurikuler memperbanyak kesempatan bagi murid untuk berinteraksi sosial dan bekerja sama

Pengembangan kegiatan ekstrakurikuler pendidikan keamanan siber dapat dilakukan melalui langkah-langkah berikut:

- **Analisis Sumber Daya:** Lakukan analisis terhadap sumber daya yang dibutuhkan,

seperti ketersediaan dana, sumber daya manusia, serta sarana dan prasarana di satuan pendidikan.

- **Identifikasi Kebutuhan Murid:** Kenali kebutuhan, potensi, bakat, dan minat murid.
- **Penetapan Bentuk Kegiatan:** Tentukan bentuk kegiatan, kompetensi yang ingin dicapai, materi pembelajaran, beban belajar, dan indikator keberhasilan.
- **Pengadaan Sumber Daya atau Penyaluran:** Upayakan pengadaan sumber daya sesuai pilihan murid atau salurkan mereka ke satuan pendidikan atau lembaga lain jika diperlukan.
- **Penyusunan Program:** Susun program ekstrakurikuler secara komprehensif.

Satuan pendidikan perlu mengintegrasikan program ekstrakurikuler keamanan siber ke dalam Rencana Kerja Sekolah. Jika program ini dikembangkan dengan sumber daya bersama, yayasan, pemerintah, atau pemerintah daerah akan memfasilitasi penggunaannya sesuai kewenangan. Sosialisasi program ini kepada murid dan orang tua/wali murid wajib dilakukan di setiap awal tahun ajaran. Sistematika program ekstrakurikuler minimal harus mencakup:

- **Rasional dan Tujuan Umum:** Penjelasan mengenai dasar dan sasaran umum ekstrakurikuler.
- **Deskripsi Ekstrakurikuler Keamanan Siber:** Uraian detail tentang kegiatan.
- **Pengelolaan:** Informasi mengenai waktu pelaksanaan dan pembinaan.
- **Pendanaan:** Sumber anggaran untuk pelaksanaan kegiatan.
- **Evaluasi:** Proses pengukuran ketercapaian tujuan.

Evaluasi ekstrakurikuler berfungsi untuk mengukur keberhasilan setiap indikator yang ditetapkan. Satuan pendidikan harus mengevaluasi indikator yang sudah maupun belum tercapai untuk kemudian melakukan perbaikan pada perencanaan siklus kegiatan berikutnya.

Penjadwalan ekstrakurikuler dirancang di awal tahun ajaran oleh pembina ekstrakurikuler, dengan supervisi dari kepala atau wakil kepala sekolah. Penting untuk memastikan jadwal ekstrakurikuler tidak mengganggu pelaksanaan intrakurikuler dan kokurikuler.

Kinerja murid dalam ekstrakurikuler keamanan siber wajib dinilai dan hasilnya dideskripsikan dalam rapor. Kriteria keberhasilan mencakup proses dan hasil capaian kompetensi murid. Penilaian dilakukan secara kualitatif.

Pelaksanaan pendidikan keamanan siber secara ekstrakurikuler tidak harus membentuk ekstrakurikuler yang baru, namun bisa juga diintegrasikan pada ekstrakurikuler yang sudah tersedia

Kegiatan ekstrakurikuler keamanan siber dapat dikembangkan melalui klub, proyek, atau kegiatan kolaboratif yang memperluas minat dan kepedulian murid. Berikut ini adalah beberapa contoh model ekstrakurikuler yang direkomendasikan:

1 Klub Anti Hoaks

Tujuan: Menumbuhkan kemampuan berpikir kritis dan keterampilan verifikasi informasi di tengah arus media sosial yang cepat.

Contoh kegiatan:

- Pelatihan mengenali berita palsu (*fact-checking workshop*).
- Kolaborasi dengan media sekolah untuk membuat rubrik "Cek Fakta Mingguan".
- Proyek "Hoax Buster": murid membuat konten edukatif berupa poster, video pendek, atau podcast.
- Kampanye digital bertema *Think Before You Share*.

Dengan adanya ekstrakurikuler semacam ini, murid mampu menjadi duta literasi digital yang berani melawan disinformasi dan menanamkan budaya berpikir kritis.

2 Pejuang Literasi (Digital)

Tujuan: Mengembangkan kesadaran dan keterampilan menjaga keamanan data pribadi serta perilaku etis di dunia maya.

Contoh kegiatan:

- *Cybersmart Day*: simulasi kejadian siber seperti *phishing* dan cara menanggulanginya.
- Pelatihan membuat sandi kuat dan mengelola jejak digital pribadi.
- Kolaborasi dengan pendidik Informatika untuk membuat modul edukasi sederhana tentang privasi digital.
- *Peer mentoring*: murid yang tergabung menjadi mentor literasi digital bagi teman sekelas atau adik kelas.

Dengan adanya ekstrakurikuler semacam ini, murid memiliki kesadaran untuk melindungi diri dan orang lain dari risiko siber, serta mampu menjadi agen perubahan di lingkungan sekolah.

D Praktik Baik Pembelajaran Kontekstualisasi Keamanan Siber

1. SD Negeri Cibubur 10 — "Melatih Keterampilan Berinternet Aman Sejak Dini"

Kompetensi Keamanan Siber:

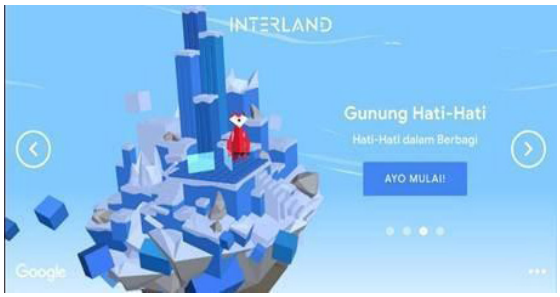
Murid memahami berbagai bentuk perilaku yang merugikan di ruang siber, seperti perundungan daring, ujaran kebencian, atau komentar kasar

SDN Cibubur 10 mengajarkan literasi digital kepada murid sekolah dasar dengan cara yang menyenangkan melalui program **"Tangkas Berinternet"**, hasil adaptasi dari **Be Internet Awesome** oleh Google.

Pembelajaran dimulai dengan penayangan video singkat tentang dasar keamanan berinternet, kemudian murid dibagi dalam kelompok kecil untuk memainkan gim **Interland**. Setiap dunia dalam permainan ini membawa pesan berbeda: berhati-hati dalam berbagi, waspada terhadap penipuan, menjaga kerahasiaan data, berperilaku sopan, dan berani bertanya jika ragu.

Pendidik berperan sebagai fasilitator yang memantik diskusi reflektif setelah misi selesai, misalnya tentang bagaimana melindungi informasi pribadi dari tautan mencurigakan. Di akhir sesi, murid mempresentasikan pelajaran yang mereka peroleh dari permainan. Pendekatan belajar sambil bermain ini terbukti efektif: murid menjadi lebih berhati-hati membagikan data pribadi, lebih kritis terhadap hoaks, dan lebih sopan berinteraksi di dunia maya.

Praktik ini membuktikan bahwa pendidikan keamanan siber bisa dilakukan sejak dini, dengan cara yang ringan namun berdampak besar.



Gambar 1. Murid-murid Praktik Langsung di Kelas

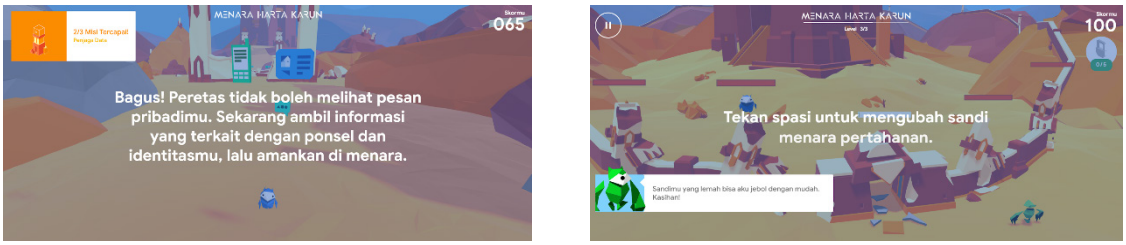
2. SD Citra Berkat Tangerang — “Keamanan Siber Sedari Dini: Dari Login hingga Kata Sandi dengan Algoritma Sederhana”

Kompetensi Pendidikan Keamanan Siber

Murid mampu memahami pentingnya pengaturan pengamanan pada perangkat dan menerapkan langkah pengamanan pada perangkat (seperti kata sandi, pola kunci, atau PIN) dengan pendampingan orang tua/wali

Di SD Citra Berkat Tangerang, pendidikan keamanan siber sudah diperkenalkan sejak kelas 1 SD melalui pengalaman sederhana yang relevan dengan kehidupan anak. Anak-anak diajarkan kebiasaan ***login*** dan ***logout*** saat menggunakan komputer di sekolah untuk melindungi data pribadi mereka. Dengan latihan rutin seperti menyalakan komputer, mengakses dokumen pribadi, dan keluar dari akun setelah selesai, murid belajar bahwa menjaga privasi di dunia digital sama pentingnya dengan menjaga ruang pribadi di dunia nyata.

Selanjutnya, mereka **mempelajari cara membuat kata sandi yang aman menggunakan algoritma sederhana**, misalnya **menggabungkan warna dan buah favorit** menjadi “BlueMango”. Tahap berikutnya, anak-anak dikenalkan dengan pembuatan kata sandi yang lebih kuat yang **memadukan huruf besar, huruf kecil, angka, dan simbol**, seperti “Ge00618*5A!BlueKiwi”. Pembelajaran dilakukan secara menyenangkan melalui simulasi di **Scratch** dan permainan edukatif seperti **Interland – Tower of Treasure** dari Google.



Gambar 2. Tangkapan Layar Interland

Selain itu, anak-anak juga **dilatih berkomunikasi secara aman di dunia digital, mengenali risiko seperti *cyberbullying*, penipuan daring, dan kebiasaan membagikan informasi pribadi secara berlebihan**. Melalui diskusi, simulasi, dan kampanye kreatif, mereka belajar bersikap bijak, melindungi diri, dan menghormati orang lain di ruang digital. Pendekatan pembelajaran yang sederhana dan konsisten ini menumbuhkan kesadaran sejak dini bahwa keamanan siber bukan hanya tentang teknologi, tetapi juga tentang tanggung jawab, etika, dan karakter di era digital melalui gim yang mengajarkan pentingnya menjaga kata sandi melalui petualangan interaktif. Melalui pendekatan gamifikasi ini, anak-anak lebih antusias belajar, memahami alasan di balik pentingnya keamanan akun, serta dapat langsung mempraktikkannya dalam kehidupan digital mereka sehari-hari.

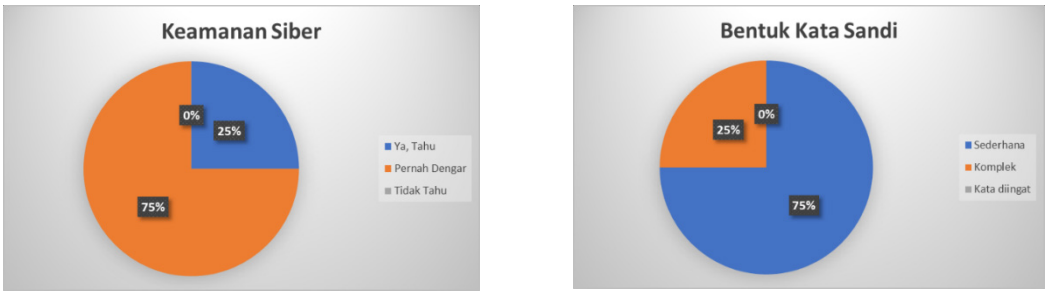
Gambar 3. Rangkaian Kegiatan terkait Keamanan Siber

3. SMP Negeri 2 Kalitidu — "Belajar Membuat Kata Sandi Aman"

Kompetensi Pendidikan Keamanan Siber:

Murid mampu menerapkan pengelolaan pengaturan keamanan dan privasi di berbagai perangkat serta akun digital yang dimiliki, (seperti mengatur izin aplikasi, mengatur mode incognito, akses kamera/file) dengan sepengetahuan orang tua/ wali

Di SMP Negeri 2 Kalitidu, pembelajaran keamanan siber dimasukkan ke mata pelajaran **Informatika** setelah pendidik menemukan bahwa 75% murid masih menggunakan kata sandi lemah seperti nama atau tanggal lahir.



Gambar 4. Hasil Survei Penggunaan Kata Sandi pada Murid SMP Negeri 2 Kalitidu

Untuk mengubah kebiasaan ini, pendidik mengembangkan pembelajaran berbasis ***Problem-Based Learning*** **(PBL)**, ***Pair Programming***, dan **PRIMM**.

Awalnya murid diminta menganalisis kasus nyata seperti peretasan akun media sosial. Mereka kemudian berdiskusi mencari solusi dan membuat algoritma kata sandi aman. Dengan *pair programming*, murid berlatih kolaborasi: satu menulis kode, satu mengamati dan memberi masukan. Pada tahap PRIMM, mereka memprediksi, menguji, dan memperbaiki kekuatan sandi menggunakan *password checker*, lalu membuat sandi sendiri dengan pemrograman visual. Sebagai hasil akhir, murid membuat **poster digital "Tips Membuat Kata Sandi Aman"** yang dipajang di sekolah dan media sosial.

Langkah Strategis Literasi Digital Keamanan Siber

Untuk mengatasi hambatan tersebut, pendidik menerapkan kombinasi tiga pendekatan: ***Problem Based Learning*** (PBL), ***Pair Programming***, dan PRIMM dalam memberikan pembelajaran Keamanan Siber melalui mata pelajaran Informatika di SMP Negeri 2 Kalitidu pada elemn Literasi Digital dan pengembangan elemen Berpikir Komputasional pada ***Pattern Recognition*** dan ***Algorithm*** untuk menyelesaikan permasalahan para murid dalam pembelajaran.

Gambar 5. Murid berkelompok menyelesaikan lembar kerja

Melalui PBL, murid diajak mengamati kasus nyata yang mereka hadapi dalam membuat kata sandi yang terlalu sederhana, serta maraknya peretasan akun media sosial yang sering terjadi di masyarakat. Dari kasus ini, mereka diminta mendiskusikan penyebab dan mencari solusi. Kegiatan ini mendorong murid berpikir kritis serta memahami bahwa kata sandi sederhana adalah salah satu penyebab utama lemahnya keamanan akun.

Gambar 6. Murid melakukan Pair Programming

Dalam proses pembelajaran Informatika, pendidik menggunakan *Pair Programming* untuk melatih kolaborasi. Murid dibagi berpasangan; satu berperan sebagai ***driver*** yang menulis pseudocode untuk membuat kata sandi kuat, sementara pasangannya sebagai ***navigator*** yang mengamati, mengoreksi, dan memberi masukan. Aktivitas ini tidak hanya meningkatkan pemahaman teknis, tetapi juga menerapkan dimensi profil lulusan komunikasi dan kolaborasi.

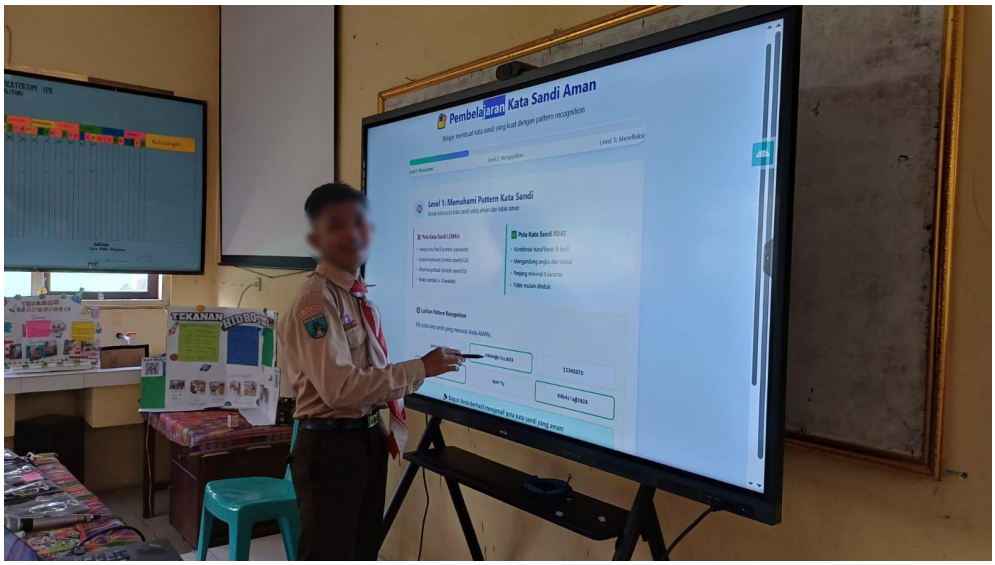
Gambar 7. Murid menguji kata sandi

Gambar 8. Murid presentasi aplikasi

Pendekatan PRIMM digunakan untuk memperkuat pembelajaran dalam pengenalan *algorithm*. Murid melakukan tahapan prediksi kekuatan sandi yang diberikan (*Predict*), kemudian menguji dengan aplikasi secara daring seperti password checker (*Run*). Setelah itu, mereka menyelidiki alasan mengapa sandi tersebut lemah atau kuat (*Investigate*), kemudian memperbaiki dengan menambahkan huruf besar, simbol, atau angka (*Modify*). Pada akhirnya, mereka membuat sendiri sandi aman sesuai pola yang telah dipelajari (*Make*) dengan menggunakan pemrograman visual.

Gambar 9. Murid membuat Poster Tips Kata Sandi Aman

Selain membuat aplikasi kata sandi berdasarkan pola yang dibuatnya, murid juga menghasilkan poster digital bertema "Tips Membuat Kata Sandi Aman" yang dipublikasikan di lingkungan sekolah atau sosial media mereka. Dengan demikian, pembelajaran tidak berhenti di ruang kelas, tetapi meluas menjadi edukasi bagi seluruh komunitas sekolah.



Gambar 10.Murid memahami bentuk Kata Sandi yang baik secara Mandiri

Pendekatan ini tidak hanya meningkatkan pemahaman teknis, tetapi juga menumbuhkan kesadaran, kreativitas, dan kebiasaan aman berinternet.

4. SMK Negeri 4 Malang — "Workshop Internal Cybersecurity Awareness"

Kompetensi Pendidikan Keamanan Siber

Murid mampu mengidentifikasi risiko siber dari aktivitas siber yang dilakukan, serta mampu menerapkan prinsip pencegahan dan pengurangan risiko tersebut

SMK Negeri 4 Malang mengembangkan program kokurikuler bertema **"Cybersecurity Awareness"** untuk menumbuhkan kesadaran keamanan siber di sekolah. Program diawali dengan pembentukan kelompok murid yang memilih topik keamanan siber sesuai minat, seperti pelindungan data pribadi atau etika digital. Setiap kelompok merancang dan melaksanakan **workshop internal** bagi murid, pendidik, dan tenaga kependidikan.

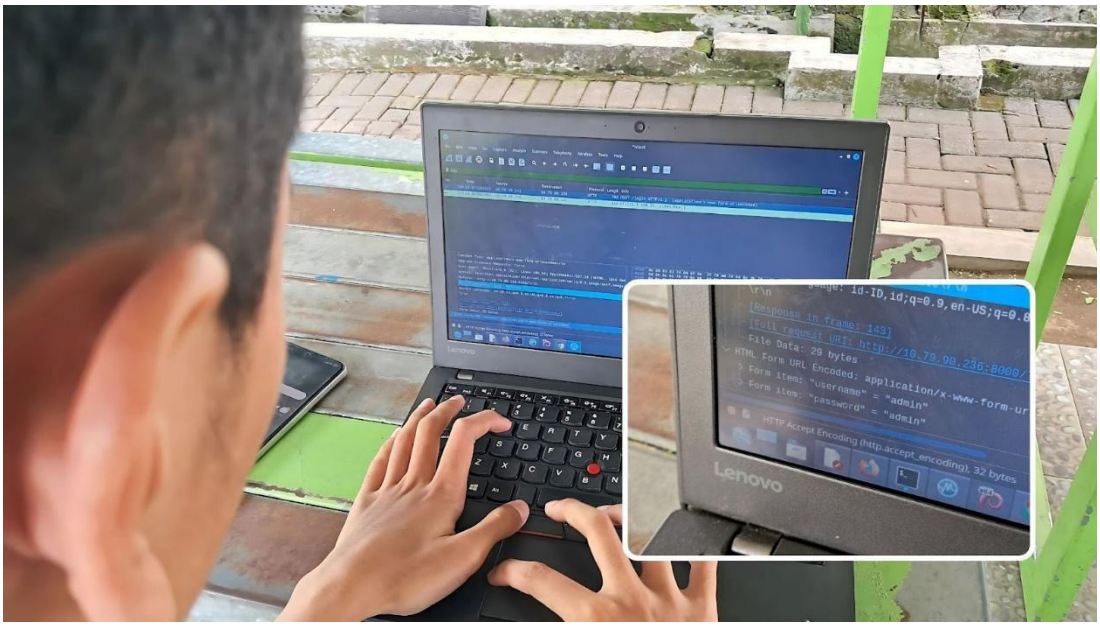
Pendidik hanya bertindak sebagai mentor, sementara murid menjadi narasumber, moderator, dan penyelenggara kegiatan. Pendekatan ini membuat murid belajar langsung mempraktikkan komunikasi, kepemimpinan, dan tanggung jawab sosial. Hasilnya, murid menjadi **agen perubahan digital** di sekolah yang menyebarkan kesadaran keamanan siber secara efektif antar-rekan sebaya.

Gambar 11.Suasana Saat Kokurikuler Cybersecurity Awareness

5. SMK Negeri 12 Malang & SMK Telkom Malang — Adaptasi Kompetensi Keamanan Siber pada Konsentrasi Keahlian TKJ

SMK Negeri 12 Malang dan SMK Telkom Sandhy Putra menjadi pelopor dalam mengintegrasikan **kompetensi keamanan siber** ke dalam **kurikulum konsentrasi keahlian Teknik Komputer dan Jaringan (TKJ)**. Inisiatif ini muncul dari kebutuhan industri digital terhadap tenaga teknis muda yang memiliki kesadaran dan kemampuan dasar di bidang keamanan siber.

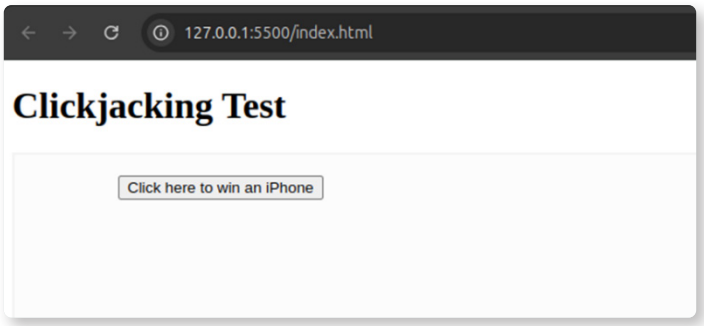
Program pembelajaran dirancang berlangsung selama **satu tahun**, dengan pendekatan berjenjang yang dibagi menjadi tiga tingkatan kompetensi (*tier*). Setiap *tier* membangun pemahaman dan keterampilan murid secara bertahap, dari kesadaran dasar hingga analisis ancaman tingkat lanjut.



Gambar 12.Murid SMKN 12 Malang Sedang Praktik Menguji Keamanan Autentikasi Pada Suatu Sistem dalam Jaringan

Tier 1 Pengenalan Keamanan Siber (Kuartal 1)

Tahapan ini fokus pada **pengetahuan dasar dan kebiasaan aman di ruang siber.** Materi meliputi: pengenalan konsep dasar keamanan siber, jenis-jenis ancaman siber seperti *phishing, malware, dan ransomware*, dasar kriptografi, serta teknik membuat kata sandi kuat. Selain itu, murid juga diperkenalkan pada dasar pemrograman *Python* untuk kebutuhan keamanan, seperti membuat skrip sederhana otomatisasi keamanan. Pendekatan yang digunakan bersifat interaktif, memadukan teori dengan simulasi sederhana, misalnya membuat kata sandi yang kuat atau mengenali email *phishing*.



Gambar 13.Tampilan Layar murid SMKN 12 Malang Pada Saat Uji *Clickjacking*

Tier 2 Keterampilan Teknis Dasar dan Respons Insiden (Kuartal 2–3)

Tahapan ini memperkuat **kemampuan teknis dan analisis praktis.**

murid diperkenalkan pada alat keamanan siber seperti *firewall*, antivirus, Wireshark, Burp Suite, SQLMap, dan Metasploit. Mereka belajar cara mendeteksi dan menanggulangi ancaman melalui simulasi insiden, serta memahami dasar **manajemen risiko siber**. Materi Python digunakan untuk latihan analisis log dan otomatisasi proses keamanan. Pendekatan praktik langsung di laboratorium menjadikan murid aktif bereksperimen dan memahami hubungan antara ancaman dan sistem pertahanan siber.

Tier 3 Analisis Ancaman dan Manajemen Keamanan (Kuartal 4)

Pada tahap akhir, murid mendalami **analisis ancaman dan pengelolaan sistem keamanan.** Mereka belajar tentang struktur website dan database untuk mengenali celah keamanan, memahami lapisan OSI dalam konteks analisis jaringan, serta melakukan *penetration testing* lanjutan secara sistematis. Kegiatan ini diakhiri dengan praktik menganalisis log sistem dan mendeteksi aktivitas mencurigakan secara langsung di lingkungan simulasi sekolah.

Sebagai bagian dari pembelajaran dunia nyata, murid juga mengikuti **praktik kerja lapangan (PKL)** di industri dan pendidikan tinggi, seperti di Universitas Brawijaya, dengan tugas mengevaluasi keamanan situs web fakultas. Program ini membentuk lulusan yang tidak hanya mahir secara teknis, tetapi juga memahami **etika profesional dan tanggung jawab digital.** Melalui integrasi kurikulum ini, SMK berhasil menyiapkan murid agar siap menghadapi tantangan keamanan siber di dunia kerja.

Gambar 14. Gambar 16 Gambar: murid SMKN 12 Malang Praktik Kerja Lapangan di Universitas Brawijaya dan Bertugas Mengevaluasi Keamanan Situs Web Fakultas di Universitas Brawijaya

BAB 5

Kemitraan dalam Pendidikan Keamanan Siber

BAB 5

Kemitraan dalam Pendidikan Keamanan Siber

A Kolaborasi Berbagai Pihak dalam Menyelenggarakan Pendidikan Keamanan Siber

Hak anak untuk memperoleh pendidikan telah dijamin dalam UUD 1945, dengan negara sebagai penanggung jawab utama penyelenggaraan sistem pendidikan nasional. Namun, proses pembelajaran anak sesungguhnya tidak hanya berlangsung di sekolah, melainkan juga di keluarga dan lingkungan sosial yang lebih luas. Oleh karena itu, pendidikan keamanan siber perlu dipahami sebagai **tanggung jawab kolektif** yang melibatkan berbagai pemangku kepentingan sesuai peran dan kapasitasnya.

Sekolah berperan sebagai **pusat pembelajaran dan koordinasi**, tempat nilai, pengetahuan, dan keterampilan keamanan siber ditanamkan secara sistematis. Meski demikian, satuan pendidikan sering menghadapi tantangan berupa keterbatasan sumber daya, kapasitas pendidik, serta kebutuhan dukungan teknis dan infrastruktur. Situasi ini menegaskan pentingnya **kemitraan multipihak yang terarah, terukur, dan saling melengkapi**, di mana kolaborasi tidak hanya dimaknai sebagai kerja sama administratif, melainkan sebagai ekosistem pembelajaran bersama.

Kemitraan dalam pendidikan keamanan siber bukan sekadar bentuk dukungan antar lembaga, tetapi merupakan **ekosistem kolaboratif yang memastikan nilai, kebiasaan, dan keterampilan keamanan siber dapat tertanam secara berkelanjutan pada murid.** Setiap pihak, mulai dari sekolah, keluarga, pemerintah, akademisi, industri, dan komunitas memiliki peran yang saling terkait, membentuk jejaring yang berpusat pada satuan pendidikan sebagai ruang tumbuh dan praktik utama.

Jenis Kemitraan	Peran Utama Mitra	Bentuk Kolaborasi yang Relevan	Manfaat untuk Sekolah & Murid
Sekolah – Orang Tua 	Menjadi teladan, pendamping, dan pengawas kebiasaan digital anak di rumah	▪ Grup komunikasi orang tua-guru ▪ Kesepakatan bersama penggunaan gawai ▪ Berbagi pengalaman tantangan aktivitas anak di ruang siber	▪ Pesan keamanan konsisten antara rumah & sekolah ▪ Kebiasaan digital sehat lebih mudah dibangun
Sekolah – Komunitas 	Memperluas edukasi digital dan kampanye positif di lingkungan sekitar	▪ Lomba konten positif ▪ Kampanye literasi digital tingkat RT/RW ▪ Kegiatan kreatif komunitas (poster, pentas, mural)	▪ Pesan keamanan siber lebih kontekstual dengan budaya lokal ▪ Membangun budaya aman di luar sekolah
Sekolah – Dunia Usaha/ Industri 	Menyediakan wawasan praktik nyata dan inspirasi profesi	▪ Sesi berbagi profesi (*career talk*) ▪ Kunjungan edukasi (*field visit*) ▪ Narasumber non-komersial	▪ Murid mengenal profesi terkait siber ▪ Pemahaman etika & tanggung jawab dalam teknologi meningkat
Sekolah – Akademisi 	Menyediakan pembaruan keilmuan, metode belajar, dan asesmen	▪ Pendampingan pengembangan modul ▪ Penelitian tindakan kelas ▪ Asesmen sederhana perilaku aman	▪ Mutu pembelajaran meningkat ▪ Guru lebih siap menerapkan pedagogi literasi digital
Sekolah – Pemerintah 	Menjamin arah kebijakan, panduan, dan dukungan teknis	▪ Sosialisasi kebijakan yang relevan ▪ Dukungan panduan keamanan siber ▪ Kanal pelaporan & koordinasi	▪ Praktik lokal selaras kebijakan nasional ▪ Sekolah punya akses informasi dan bimbingan resmi

Keterhubungan dan Sinergi Ekosistem

Setiap bentuk kemitraan tidak berdiri sendiri. Sekolah menjadi simpul utama yang menghubungkan pemerintah, akademisi, industri, komunitas, dan keluarga dalam satu **ekosistem pembelajaran keamanan siber** yang hidup dan berkelanjutan.

Kolaborasi lintas aktor ini membentuk sistem pendidikan keamanan siber yang **berlapis dan resilien**, di mana setiap pihak berkontribusi sesuai kapasitasnya dalam membangun kesadaran dan ketangguhan digital murid. Hasil akhirnya bukan sekadar proteksi pasif terhadap risiko, tetapi pembentukan **ketahanan ruang siber sejak dini** kemampuan anak mengenali risiko, melindungi diri, serta memulihkan kepercayaan diri ketika menghadapi ancaman.

Dengan demikian, pendidikan keamanan siber berbasis kemitraan multipihak berfungsi sebagai **"pagar berlapis"** yang melindungi sekaligus memberdayakan. Pendekatan ini memperkuat posisi pendidikan keamanan siber sebagai bagian integral dari sistem pendidikan nasional, yang bertujuan menumbuhkan generasi cerdas, kritis, berdaya saing, dan bertanggung jawab dalam ruang siber.

B Prinsip, Etika, dan Kaidah Kemitraan

Kemitraan antarpemangku kepentingan merupakan salah satu strategi untuk mempercepat tercapainya tujuan pendidikan keamanan siber. Melalui kolaborasi yang sehat dan terarah, satuan pendidikan memperoleh dukungan berupa pengetahuan, fasilitas, pengalaman dan penguatan budaya aman di ruang siber. Kemitraan harus dibangun tidak hanya berdasarkan kebutuhan, tetapi juga mematuhi prinsip, etika, dan kaidah berikut:

Prinsip Kemitraan	
Kolaboratif	Semua pihak bekerja sama, berinteraksi secara aktif dan berfokus dalam mencapai tujuan pendidikan keamanan siber.
Inklusif	Semua pemangku kepentingan berhak terlibat tanpa memandang perbedaan status atau latar belakang.
Akuntabel	Setiap pihak bertanggung jawab atas kontribusi, peran, dan tindakannya, serta transparan dalam pelaporan kegiatan.
Berkelanjutan	Kemitraan dirancang jangka panjang, bukan kegiatan sekali lewat.
Sinergis	Setiap pihak saling mendukung dengan menggabungkan keahlian, sumber daya dan pengalaman.

Etika Kemitraan

Etika	Pesan Utama
Pelindungan Data Murid	Mitra tidak mengambil, menyimpan, atau memindahkan data tanpa izin.
Persetujuan Orang Tua	Penggunaan foto, rekaman, atau partisipasi murid harus disetujui orang tua.
Transparansi Tujuan	Semua pihak menyampaikan tujuan kegiatan secara jujur dan terbuka.
Tanpa Kepentingan Komersial	Tidak boleh ada promosi produk, platform, atau agenda industri terselubung.

Kaidah Kemitraan

Do (Yang Boleh Dilakukan)

- ✓ Menetapkan tujuan kegiatan yang jelas dan relevan.
- ✓ Menyajikan materi yang netral, aplikatif, dan sesuai usia murid.
- ✓ Menelaah setiap materi dari mitra sebelum digunakan.
- ✓ Mengelola kegiatan berdasarkan kebutuhan sekolah, bukan kepentingan sponsor.

Don't (Yang Tidak Boleh Dilakukan)

- ✗ Memasarkan aplikasi, platform, atau merek tertentu.
- ✗ Menggunakan data murid tanpa formulir persetujuan.
- ✗ Memberikan materi yang mengandung opini, ketakutan berlebih, atau tidak bisa diverifikasi.
- ✗ Mengumpulkan data murid untuk kepentingan lain di luar kegiatan edukasi.

C Mitra Komunitas, Akademisi, Dunia Usaha, dan Lembaga Pemerintah

1 Komunitas

Komunitas literasi digital berperan penting dalam pendidikan keamanan siber di sekolah karena dapat menjembatani kesenjangan antara pengetahuan teknis dan penerapan perilaku yang aman melalui pendekatan yang interaktif, kreatif, dan berbasis jejaring relawan. Komunitas berfokus pada pengembangan etika digital dan kemampuan berpikir kritis murid, yang sangat vital dalam menghadapi ancaman siber yang kompleks seperti hoaks, penipuan *online*, dan perundungan daring. Interaksi sebaya yang difasilitasi komunitas juga membantu menanamkan kebiasaan aman secara berkelanjutan pada murid.

Masing-masing komunitas literasi digital punya kekhasannya masing-masing, ada yang fokus dalam bidang tertentu, misalnya antihoaks, pelindungan anak dari *cyberbullying*, dan ada komunitas yang fokus di satu area tertentu, dan ada juga yang punya jejaring relawan hingga ke daerah.

Tahukah Anda

Gerakan Nasional Literasi Digital (GNLD) SIBERKREASI (siberkreasi.id) adalah sebuah gerakan yang diinisiasi oleh Kementerian Komunikasi dan Informatika bersama dengan lintas komunitas literasi digital yang saat ini beranggotakan lebih dari 100 komunitas yang aktif dalam melakukan edukasi literasi digital, seperti Kumpulan Emak Blogger (KEB), Relawan TIK (RTIK), Masyarakat Antifitnah Indonesia (MAFINDO), ICTWatch, Japelidi, dan banyak lainnya. Gerakan ini memiliki jejaring relawan yang luas, anggotanya juga memiliki banyak sumberdaya baik kurikulum dan materi yang bisa mendukung pendidik di sekolah.

Selain itu ada aliansi Indonesia Child Online Protection (ID-COP, idcop.org) yang terdiri dari beberapa organisasi seperti ECPAT, Yayasan Sejiwa, ICTWatch, Save The Children dan lainnya yang fokus dalam issue pelindungan anak di ruang siber. Aliansi ini memiliki banyak materi yang sangat bermanfaat untuk digunakan pendidik memberikan pengetahuan keamanan siber di sekolah.

Komunitas literasi digital menyediakan dukungan yang dapat langsung dimanfaatkan sekolah, baik untuk kegiatan pembelajaran, penguatan budaya aman siber, maupun pemberdayaan orang tua. Bentuk dukungan ini dapat diakses secara fleksibel sesuai kapasitas sekolah.

Jenis Dukungan Komunitas	Contoh Implementasi Operasional di Sekolah
Jejaring *Trainer* Literasi Digital Pelatih/relawan yang memiliki kompetensi literasi digital dan keamanan siber.	▪ Mengisi kelas tematik/MPLS tentang keamanan siber. ▪ *Micro-training* singkat untuk guru (20–30 menit). ▪ Pendampingan sekolah menyusun aturan penggunaan gawai.
Modul & Materi Terstruktur Paket materi siap pakai yang aman secara pedagogis dan bebas promosi.	▪ Modul dasar privasi, etika digital, jejak digital. ▪ RPP mini 1 jam pelajaran untuk guru. ▪ Lembar informasi untuk orang tua.
Permainan Edukatif Media belajar non-digital yang membuat murid memahami konsep keamanan siber secara menyenangkan.	▪ *Boardgame* tentang hoaks dan jejak digital. ▪ Ular tangga mengenai keamanan akun. ▪ *Role-play* "izin/tidak izin" atau "aman/tidak aman".
Konten Multimedia Materi visual dan audio untuk memperkuat budaya digital aman.	▪ Poster etika digital dipasang di kelas. ▪ Video pendek tentang privatasi & keamanan akun. ▪ Infografis kampanye untuk grup WhatsApp sekolah.
Pendampingan Program Kolaborasi jangka menengah untuk membangun kebiasaan digital aman.	▪ Penyusunan SOP penggunaan perangkat di sekolah. ▪ Program "Pekan Aman Siber" bersama warga sekolah. ▪ Evaluasi triwulan perilaku digital murid.

Berikut ini adalah beberapa komunitas literasi digital yang dapat menjadi mitra sekolah dalam menyelenggarakan pendidikan keamanan siber:

Tabel 7 Komunitas Literasi Digital di Indonesia

Nama Komunitas	Fokus Bidang	Website/Media Sosial
SIBERKREASI	Literasi Digital	siberkreasi.id http://s.id/modul4pilar https://linktr.ee/4pilarcabe
MAFINDO	Literasi Digital & Antihoaks	mafindo.or.id turnbackhoax.id tularnalar.id
ICTWatch	Literasi Digital	internetsehat.id https://linktr.ee/internetsehat
ECPAT	Literasi Digital dan Perlindungan Anak dari Eksploitasi Seksual	www.ecpatindonesia.org
Sejiwa	Literasi Digital dan Kesehatan Mental Anak dan Keluarga	sejiwa.org
RTIK	Literasi Digital dan Pemberdayaan Digital	relawantik.or.id
Kelompok Emak Blogger	Literasi Digital dan Pemberdayaan Perempuan di Ruang siber	emak2blogger.com
Save The Children	Perlindungan Anak	savethechildren.or.id
Center for Digital Society	Literasi Digital	digitalsociety.id
JAPELIDI	Literasi Digital	japelidi.id

Praktik Baik

Kolaborasi Sekolah dengan Komunitas

SMP 26 Al Azhar Yogyakarta termasuk yang sangat serius untuk mencegah muridnya menjadi korban atau pelaku *cyberbullying*, karenanya pendidik sekolahnya mencari mitra yang bisa membantu untuk mengedukasi muridnya tentang dampak *cyberbullying* sekaligus cara penanganan jika terlanjur menjadi korban.

Pendidik kemudian mencari kontak komunitas yang punya gerak dalam isu keamanan siber, dan mengundang komunitasnya untuk menyelenggarakan sesi belajar untuk murid baru. Karena sekolahnya di Jogja, ia mencari referensi komunitas yang aktif di Jogja, dan ketemu dengan salah satu komunitas yang dikenal punya kompetensi dalam *cyberbullying*.

Maka di bulan Juli 2023, pada hari Masa Pengenalan Lingkungan Sekolah (MPLS) di tahun ajaran 2023/2024, semua murid baru dikumpulkan di aula. Komunitas menyajikan materi dengan interaktif dan dibantu dengan video penjelasan dan permainan tentang pentingnya untuk tidak menjadi korban atau pelaku *cyberbullying*.

Setelah sesi interaksi selesai, kemudian pendidik meminta semua murid untuk menandatangani pakta integritas anti *cyberbullying*.

Pendekatan kemitraan seperti ini akan bisa menjadikan aktivitas pendidikan siber bisa lebih menarik karena pendidik akan bisa didampingi oleh pegiat literasi digital yang umumnya memiliki banyak metode, konten video menarik, permainan, sehingga proses pembelajarannya bisa menyenangkan dan mudah dipahami.

Dan karena biasanya materi, video, permainan, yang dibuat oleh komunitas boleh dibagikan kepada pendidik, sehingga pendidik pun akhirnya punya referensi tambahan jika ingin menyampaikan materi tentang keamanan siber di kelasnya.

2 Akademisi

Perguruan tinggi yang memiliki jurusan atau program studi terkait keamanan siber, dapat menjadi salah satu mitra strategis. Selain itu, adanya **Program Kampus Berdampak**[1] juga memungkinkan mahasiswa untuk mengajar keamanan siber di sekolah sebagai bagian dari pengabdian masyarakat. Beberapa aktivitas yang dapat dilakukan dengan menggandeng kampus antara lain:

Aspek	Bentuk Dukungan Akademisi	Contoh Implementasi Operasional di Sekolah
Pengembangan Materi Ajar	Kolaborasi kampus-sekolah untuk menyusun modul keamanan siber sesuai jenjang	Modul dasar keamanan siber untuk SD dan SMP
Materi lanjutan (privasi, jejak digital, keamanan akun) untuk SMA		
Kampus membantu membuat materi interaktif (slide, video pendek, lembar aktivitas)		
Pelatihan Pendidik & Murid	Pelatihan literasi digital dan keamanan siber serta sertifikasi dari kampus	*Workshop* guru tentang keamanan akun, privasi, dan manajemen kelas digital
Sertifikasi pelatihan dari kampus bagi guru		
Mahasiswa terlatih menjadi mentor mingguan untuk pendidik/murid		
Kegiatan Ekstrakurikuler	Dukungan kegiatan untuk meningkatkan minat murid terhadap keamanan siber	Klub Keamanan Siber sekolah dengan pendampingan mahasiswa
Mini-hackathon, lomba poster keamanan, atau cerdas cermat digital		
Seminar dan lokakarya yang menghadirkan dosen dan praktisi industri		

1 Program Kampus Berdampak merupakan inisiatif Kementerian Pendidikan, Sains, dan Teknologi untuk mentransformasi perguruan tinggi agar lebih berperan aktif dalam pembangunan nasional dan mencapai visi Indonesia Emas 2045. Program ini mendorong kampus untuk memberikan manfaat nyata bagi masyarakat, industri, dan dunia pendidikan dengan fokus pada aplikasi ilmu pengetahuan, teknologi, dan inovasi untuk menghasilkan perubahan sosial dan ekonomi yang positif.

Aspek	Bentuk Dukungan Akademisi	Contoh Implementasi Operasional di Sekolah
***Roadshow* Kampus–Sekolah**	Program kunjungan kampus ke sekolah dengan materi edukasi keamanan siber	*Roadshow* pada Masa Pengenalan Lingkungan Sekolah (MPLS)
Sesi berbagi oleh dosen/mahasiswa tentang etika digital dan risiko siber		
Kunjungan berkala difasilitasi oleh dinas pendidikan		
Pendampingan Berkelanjutan	Akademisi sebagai mitra jangka panjang untuk penguatan budaya aman digital	Dosen sebagai pembina program literasi digital sekolah
Kolaborasi penelitian tindakan kelas tentang perilaku digital murid		
Review rutin materi keamanan siber agar tetap mutakhir		

3 Industri/Dunia Usaha

Kemitraan antara sekolah dan industri memiliki peran penting dalam memperkuat ekosistem pendidikan keamanan siber di tingkat pendidikan dasar dan menengah. Dunia industri tidak hanya memiliki pengalaman langsung menghadapi ancaman siber, tetapi juga memiliki sumber daya edukatif yang dapat membantu sekolah menanamkan pemahaman dan kebiasaan aman di ruang siber secara kontekstual dan menarik bagi anak-anak maupun remaja.

Bagi sekolah, kemitraan ini dapat memperkaya proses belajar-mengajar dengan menghadirkan contoh nyata penerapan keamanan siber di dunia kerja dan kehidupan sehari-hari. Sementara bagi industri, kolaborasi dengan sekolah menjadi wujud nyata tanggung jawab sosial untuk menumbuhkan generasi muda yang melek digital, etis, dan tangguh terhadap ancaman siber.

Kemitraan ini dapat dilakukan tidak hanya oleh perusahaan keamanan siber, tetapi juga oleh perusahaan teknologi, telekomunikasi, perbankan digital, maupun startup edukasi yang memiliki komitmen terhadap literasi dan keamanan siber anak.

Beberapa bentuk program kemitraan yang dapat dikembangkan antara sekolah dan industri antara lain:

Kategori Dukungan	Bentuk Dukungan Ringkas	Contoh Implementasi di Sekolah
Konten Edukatif & Media Pembelajaran	Penyediaan video, poster, buku bergambar, permainan interaktif.	Video pendek tentang kata sandi aman; poster anti-hoaks; modul cerita untuk jenjang SD.
Pelatihan Pendidik & Literasi Digital Aman	*Workshop* keamanan siber, etika digital, dan perlindungan data.	Pelatihan "Keamanan Digital untuk Guru"; sesi praktik mengatur privasi akun.
Program Edukasi & Kampanye Bersama	Kampanye tematik tentang keamanan siber dan literasi digital.	"Bulan Aman Digital", lomba poster/komik, kelas tematik anti-hoaks.
Kunjungan Edukasi & Kelas Inspirasi	Kunjungan murid ke perusahaan atau praktisi datang ke sekolah.	Tur kantor TI; sesi berbagi profesi (*ethical hacker, cyber analyst*).
Program CSR / Adopsi Sekolah	Dukungan jangka panjang berupa sarana, platform aman, atau pembinaan.	Penyediaan perangkat, akses platform belajar aman, *sponsorship* kompetisi literasi digital.

Melalui kemitraan yang inklusif dan berkelanjutan, sekolah tidak hanya memperkuat kompetensi keamanan siber murid, tetapi juga membangun budaya digital yang sehat di lingkungan pendidikan. murid tidak hanya diajarkan untuk "berhati-hati" di dunia maya, tetapi juga untuk **bertanggung jawab, kritis, dan berempati** terhadap sesama pengguna ruang siber.

Tabel 8 Program Edukasi Keamanan siber dari Perusahaan Teknologi

Nama Industri / Mitra	Bentuk Kontribusi / Dukungan	Sasaran Jenjang Pendidikan	Contoh Kegiatan / Program
Palo Alto Networks (bersama IWCS)	Pengembangan konten edukatif, pelatihan pendidik, pendampingan sekolah	SD, SMP, SMA	*CyberSafe Kids Indonesia* – menyediakan modul pembelajaran, video edukatif, dan pelatihan pendidik terkait keamanan siber anak.
Google Indonesia	Pelatihan pendidik, literasi digital, kampanye anti-hoaks	SD, SMP, SMA	*pendidik Cakap Digital dan #BersamaHadapiHoaks* – pelatihan pendidik dan kegiatan di sekolah untuk mengenali hoaks serta melindungi data pribadi.
Meta Indonesia (Facebook, Instagram, WhatsApp)	Edukasi literasi digital dan etika media sosial	SMP, SMA	*Aman Bersama META* – roadshow ke sekolah-sekolah dengan pelatihan dan simulasi aman berinteraksi di media sosial.
Telkom Indonesia	Dukungan infrastruktur digital aman, konten edukasi	SD, SMP	*Smart School* – menyediakan jaringan internet aman, konten edukasi digital, dan pembiasaan perilaku aman daring.
Indosat Ooredoo Hutchison	Kampanye literasi dan keamanan internet	SD, SMP, SMA	*Internet Sehat dan Aman (INSAN)* – sosialisasi dan pelatihan langsung di sekolah tentang penggunaan internet yang positif dan aman.
Huawei Indonesia	Pelatihan teknologi dan keamanan siber, program beamurid	SMA, SMK	*Seeds for the Future* – memperkenalkan dasar keamanan siber dan karier digital melalui pelatihan dan kunjungan industri.

Nama Industri / Mitra	Bentuk Kontribusi / Dukungan	Sasaran Jenjang Pendidikan	Contoh Kegiatan / Program
Xynexis Indonesia	Edukasi profesional, kelas inspirasi, simulasi keamanan siber	SMA, SMK	*Cybersecurity Roadshow* – menghadirkan praktisi keamanan siber ke sekolah dan simulasi penanganan insiden siber sederhana.
CyberArmyID	Edukasi dasar keamanan data dan tanggung jawab digital	SMP, SMA	*Kelas Inspirasi Cyber Awareness* – pelatihan interaktif untuk mengenali ancaman siber dan praktik keamanan siber.
Microsoft Indonesia	Edukasi keamanan akun dan privasi digital	SD, SMP	*Digital Civility Campaign* – sosialisasi perilaku sopan di dunia digital dan pelindungan identitas daring bagi anak-anak.
Tokopedia & Gojek (GoTo Group)	Program CSR edukatif tentang keamanan transaksi dan privasi	SMP, SMA	*Cerdas Bertransaksi Digital* – pelatihan langsung di sekolah tentang keamanan berbelanja dan etika digital.

4 Lembaga Pemerintah dan Organisasi Internasional

Sekolah juga dapat membangun kemitraan dengan berbagai **instansi dan lembaga pemerintahan** untuk memperkuat penyelenggaraan pendidikan keamanan siber. Instansi pemerintah memiliki peran penting sebagai fasilitator kebijakan, penyedia sumber daya, dan pendamping teknis agar sekolah memiliki kemampuan yang memadai dalam melaksanakan pembelajaran keamanan siber secara terarah dan berkelanjutan.

Kemitraan dengan Lembaga Pemerintah

Kerja sama antara sekolah dan lembaga pemerintah bersifat saling melengkapi. Pemerintah pusat, daerah, dan lembaga teknis memiliki kapasitas dalam hal **kebijakan, riset, serta infrastruktur teknologi**, sementara sekolah menjadi garda terdepan dalam membentuk perilaku aman di ruang siber. Melalui kemitraan ini, pembelajaran keamanan

siber tidak hanya menjadi pengetahuan tambahan, tetapi terintegrasi dalam keseharian murid dan lingkungan sekolah.

Beberapa contoh bentuk kemitraan dan program yang dapat dilakukan antara sekolah dan lembaga pemerintahan antara lain:

Kategori Mitra Pemerintah	Bentuk Dukungan Utama	Contoh Implementasi di Sekolah
Dinas Pendidikan Daerah	Koordinasi pelaksanaan pendidikan keamanan siber. Pelatihan pendidik & pengawas. Program apresiasi sekolah aman siber.	*Program Sekolah Aman Siber Daerah.* Pelatihan guru TIK & wali kelas tentang integrasi topik keamanan siber. Bimtek implementasi kurikulum bersama lembaga teknis (BSSN/ Kominfo).
Diskominfo (Dinas Komunikasi & Informatika Daerah)	Literasi digital & edukasi keamanan data pribadi. Dukungan teknis publikasi & kampanye digital. Penguatan infrastruktur & sistem pelaporan insiden sederhana.	Sosialisasi keamanan data pribadi dan simulasi hoaks. Pembuatan portal keamanan siber sekolah atau *sistem incident reporting*. Kampanye "Aman di Dunia Maya" melalui kanal resmi Diskominfo.
Lembaga Teknis Nasional (BSSN)	Edukasi keamanan siber nasional untuk sekolah. Pelatihan guru melalui akademi siber. Materi pembelajaran & panduan praktis.	*Cyber Education Roadshow,* sosialisasi keamanan akun & kata sandi. Program *CyberSafe Kids* di sekolah. Pelatihan pendidik melalui jejaring lembaga pelatihan siber nasional.
TTIS / CSIRT Daerah (Tim Tanggap Insiden Siber)	Pendampingan penanganan insiden siber. Simulasi keamanan & audit jaringan sederhana. Pembinaan kelompok sadar siber.	Simulasi *phishing* atau kebocoran data murid. *Cyber Clinic* berkala untuk mengevaluasi keamanan jaringan sekolah. Pembentukan *Kelompok Sadar Siber (KSS)* sebagai ekstrakurikuler.

Kategori Mitra Pemerintah	Bentuk Dukungan Utama	Contoh Implementasi di Sekolah
Polri, Kejaksaan, KPAI, KemenPPPA	Penguatan aspek hukum & perlindungan anak digital. Edukasi etika dan keamanan digital.	"Polisi Sahabat Murid di Dunia Digital". Kelas anti-perundungan siber dan pencegahan eksploitasi daring.
Pemerintah Desa / Kecamatan	Dukungan komunitas & fasilitas belajar digital aman. Penguatan ekosistem keamanan siber lokal.	Program "Sekolah Desa Digital Aman" untuk warga sekitar. Penyediaan digital hub ramah anak & ruang edukasi publik.

Berikut adalah contoh kegiatan kemitraan yang dilakukan bersama antara sekolah dengan beberapa lembaga pemerintahan:

Tabel 9 Contoh kegiatan kemitraan antara sekolah dengan lembaga pemerintahan

Judul Kegiatan	Lembaga Pemerintah Mitra	Pelaksanaan & Keterlibatan Sekolah/ Guru	Substansi Kemitraan (Fokus Keamanan Siber/Literasi Digital)
Literasi *Cyber Security*	BSSN	Kegiatan bersama BSSN dan sekolah-sekolah; guru TIK dan siswa aktif sebagai peserta dan co-trainer; sekolah menyiapkan ruang praktik.	Pelatihan dasar keamanan siber, pengelolaan kata sandi, keamanan akun belajar.id, serta simulasi hoaks.
Basic Cyber Security untuk Pelajar Sekolah Menengah di SMKN 1 Seyegan	BPSDMP Kominfo Yogyakarta	Pelatihan langsung di sekolah; fasilitator dari Kominfo; sekolah menyiapkan lab dan peserta.	Pengenalan ancaman siber, pelindungan data pribadi, keamanan jaringan dasar.

Judul Kegiatan	Lembaga Pemerintah Mitra	Pelaksanaan & Keterlibatan Sekolah/ Guru	Substansi Kemitraan (Fokus Keamanan Siber/Literasi Digital)
Thematic Academy – *Basic Cyber Security* Batch Surabaya	BPSDMP Kominfo	Siswa SMK dan guru TIK mengikuti pelatihan di kantor BPSDMP dan sekolah; modul dibagikan untuk pembelajaran lanjutan.	Literasi digital aman, pengelolaan kata sandi, etika siber, dan proteksi identitas digital.
Diskominfo *Goes to School* di SMP 10 Makassar	Diskominfo Kota Makassar	Program rutin kunjungan Kominfo ke sekolah; sekolah menjadi tuan rumah kegiatan dan melibatkan guru BK serta wali kelas.	*Cyberbullying*, *phishing*, keamanan data pribadi, literasi media sosial aman.
Sosialisasi Literasi Digital di SMPN 6 Wadaslintang	Diskominfo Kabupaten Wonosobo	Diselenggarakan saat MPLS dengan dukungan guru TIK; Kominfo menyampaikan materi dan simulasi langsung kepada siswa.	Internet sehat, bahaya konten negatif, judi online, dan etika digital.

Kemitraan dengan lembaga pemerintahan memberikan keuntungan ganda. Bagi sekolah, kemitraan membantu memperkuat kapasitas pendidik dan menumbuhkan budaya aman di ruang siber lingkungan pendidikan. Sementara bagi pemerintah, kegiatan ini menjadi bagian dari upaya memperluas literasi keamanan siber masyarakat secara berjenjang dan berkelanjutan.

Pada akhirnya, melalui jejaring kerja sama yang kuat antara sekolah dan lembaga pemerintah, akan terbangun **ekosistem pendidikan keamanan siber nasional yang adaptif, inklusif, dan berkelanjutan**, di mana seluruh elemen bangsa berperan aktif melindungi generasi muda di ruang siber.

Kemitraan dengan Organisasi Internasional

Selain bekerja sama dengan pemerintah, sekolah juga dapat bermitra dengan organisasi internasional yang memiliki fokus pada pendidikan, pelindungan anak, dan literasi digital. Lembaga seperti UNICEF, UNESCO, ChildFund, Save the Children, atau Plan International telah banyak berperan dalam memperkuat kapasitas sekolah dalam menghadapi tantangan ruang siber yang dinamis.

Melalui kemitraan ini, sekolah memperoleh dukungan teknis, sumber daya, dan akses terhadap praktik baik global yang relevan dengan konteks lokal. Bentuk kegiatan dapat berupa pelatihan guru, penyusunan modul pembelajaran aman di internet, kampanye literasi digital dan anti-perundungan, hingga program advokasi pelindungan data anak di sekolah.

Organisasi internasional biasanya bekerja bersama pemerintah daerah, dinas pendidikan, dan komunitas, maupun akademisi untuk memastikan setiap kegiatan menyesuaikan dengan kebutuhan lokal dan nilai-nilai budaya setempat. Dengan pendekatan ini, sekolah tidak hanya menjadi penerima manfaat, tetapi juga mitra aktif dalam membangun budaya aman di ruang siber.

Kemitraan ini juga membuka jalan bagi sekolah untuk menjadi bagian dari jaringan pendidikan global, memperluas wawasan murid dan pendidik, serta menumbuhkan nilai solidaritas digital lintas negara yang penting untuk membangun generasi yang tangguh, kritis, dan bertanggung jawab di ruang siber. Berikut ini adalah beberapa contoh program kemitraan yang sudah pernah dilakukan bersama dengan organisasi internasional di Indonesia:

Tabel 10 Contoh kegiatan kemitraan antara sekolah dengan organisasi internasional

Judul Kegiatan / Program	Organisasi Internasional	Deskripsi Kemitraan	Substansi Kemitraan
SAFE4C — Strengthening Safe & Friendly Environments for Children Online	UNICEF Indonesia (project SAFE4C)	Proyek nasional bersama pemerintah untuk memperkuat pencegahan dan respons terhadap eksploitasi seksual anak online; melibatkan pelatihan, penguatan layanan, dan dukungan kebijakan.	Literasi & perlindungan anak online; pelatihan guru/pendamping; dukungan kebijakan daerah; sistem rujukan dan respons korban.
	https://safeonline.global/unicef-indonesia/		

Judul Kegiatan / Program	Organisasi Internasional	Deskripsi Kemitraan	Substansi Kemitraan
Gateways Study Visits & Digital Education Support	UNICEF & UNESCO (Gateways initiative)	Kunjungan studi dan sharing praktik untuk pembuat kebijakan dan praktisi; pendampingan penyusunan konten pembelajaran digital.	Penyediaan konten pembelajaran digital aman; peningkatan kapasitas guru; pembelajaran digital yang responsif dan aman.
	https://www.unicef.org/digitaleducation/safety; https://www.unicef.org/digitaleducation/gateways-study-visit-indonesia		
Swipe Safe, Kampanye Web Safe & Wise	ChildFund International (ChildFund Indonesia)	Penguatan Ekosistem Perlindungan Anak Offline & Online; Kampanye, Pelatihan, Pengembangan Materi/Modul Keamanan Online/ Anti *Cyberbullying*; Pelatihan Guru.	Edukasi Pencegahan Perundungan, Modul Pembelajaran & Pelatihan Guru, Kampanye Kesadaran dan Dukungan Psikososial bagi Anak dan Guru/Pengasuh Utama.
	https://childfund.id/publikasi/download/38; https://app.swipesafe.org/4GaTKVE9zm1lPiSO9Fvq8qtE/		
First Click — Modul & E-Learning Perlindungan Anak di Era Digital	Save the Children (dengan KPPPA di Indonesia)	Peluncuran modul & platform e-learning, uji coba di sejumlah sekolah/daerah; pelatihan pendidik.	Modul perlindungan anak digital: manajemen kasus, kompetensi digital anak & orang muda, kebijakan lembaga, pengasuhan digital.
	https://savethechildren.or.id/artikel/melindungi-anak-di-era-digital-save-the-children-dan-kpppa-luncurkan-modul-dan-e-learning-program-first-click.		

Judul Kegiatan / Program	Organisasi Internasional	Deskripsi Kemitraan	Substansi Kemitraan
Ready4Security / Cybersecurity Skills Initiative	Microsoft (regional program dengan mitra lokal)	Program skilling/ bootcamp dan training-of-trainers untuk pengajar & pemuda; dukungan kurikulum & beasiswa sertifikasi.	Pelatihan hardskill keamanan siber, pengembangan kurikulum, pelatihan pendidik dan talenta muda; dukungan sertifikasi dasar.
	https://news.microsoft.com/id-id/2023/06/16/empowering-indonesias-digital-defenses-against-cybercrime/; https://blogs.microsoft.com/on-the-issues/2023/04/19/cybersecurity-skills-initiative-expansion-nonprofits/.		
ASEAN Foundation + Microsoft — Cybersecurity Skilling (ASEAN)	ASEAN Foundation & Microsoft (program regional yang meliputi Indonesia)	Pengembangan kurikulum, TOT untuk pendidik/ fasilitator, pelatihan lanjutan di negara ASEAN termasuk Indonesia.	Capacity building: TOT bagi edukator, materi belajar cybersecurity yang dapat diadaptasi untuk sekolah/SMK.
	https://aseanfoundation.org/asean-foundation-and-microsofts-cybersecurity-skilling-programme-benefited-24886-people-in-asean/		

D Menemukan dan Menjalin Kemitraan Strategis

Kemitraan dalam pendidikan keamanan siber diperlukan untuk memastikan bahwa program pembelajaran berjalan secara selaras dengan prioritas sekolah, kebutuhan murid, serta kapasitas pendidik. Dengan adanya kemitraan yang terkelola dengan baik, sekolah dapat memperluas akses terhadap sumber belajar, pelatihan, pendampingan, serta dukungan teknis yang relevan dengan perkembangan teknologi dan dinamika risiko digital.

Kemitraan dapat dimulai dari inisiatif sekolah maupun inisiatif mitra eksternal, seperti dinas pendidikan, perguruan tinggi, komunitas digital, industri teknologi, maupun lembaga bantuan hukum dan paralegal komunitas. Terlepas dari siapa yang memulai, kemitraan yang efektif harus memiliki tujuan yang jelas, mekanisme pelaksanaan yang transparan, dan komitmen terhadap keberlanjutan.

1 Kemitraan yang Diinisiasi oleh Sekolah

Ketika sekolah mengambil peran sebagai penggerak kolaborasi, proses kemitraan perlu disusun secara sistematis agar dapat menghasilkan kegiatan yang relevan dan memenuhi kebutuhan murid. Berikut tahapan umum yang dapat digunakan oleh sekolah.

Tahapan	Deskripsi Kegiatan	Pihak yang Terlibat	Keluaran yang Diharapkan
1. **Identifikasi Kebutuhan Sekolah**	Sekolah melakukan analisis kebutuhan pembelajaran keamanan siber berdasarkan kondisi murid, kapasitas pendidik, serta ketersediaan sarana prasarana digital.	Kepala sekolah, pendidik TIK, komite sekolah	Dokumen pemetaan kebutuhan dan prioritas program.
2. **Pembentukan Tim Penggerak**	Sekolah membentuk tim lintas fungsi untuk menyiapkan rencana kemitraan dan memastikan koordinasi pelaksanaannya.	Pendidik, tenaga kependidikan, komite sekolah	Tim penggerak serta rencana awal kolaborasi.
3. **Pemilihan Mitra Potensial**	Tim mengidentifikasi mitra relevan, seperti dinas pendidikan, perguruan tinggi, komunitas digital, industri, lembaga bantuan hukum, atau paralegal komunitas.	Tim penggerak, kepala sekolah	Daftar mitra potensial dan jenis dukungan yang dibutuhkan.
4. **Penyusunan Rencana Kegiatan**	Sekolah menginisiasi diskusi awal dengan calon mitra untuk menentukan tujuan bersama, metode pelaksanaan, jadwal, dan mekanisme evaluasi.	Sekolah dan mitra eksternal	Rencana aksi kegiatan kemitraan (program matrix).

Tahapan	Deskripsi Kegiatan	Pihak yang Terlibat	Keluaran yang Diharapkan
5. **Pelaksanaan Kegiatan**	Pelaksanaan dilakukan sesuai kesepakatan, seperti pelatihan, simulasi keamanan siber, kelas inspirasi, atau kampanye digital aman.	Sekolah dan mitra	Terselenggaranya kegiatan yang partisipatif dan aman.
6. **Evaluasi dan Tindak Lanjut**	Sekolah bersama mitra melakukan evaluasi dampak dan menyusun rencana keberlanjutan program.	Sekolah dan mitra	Laporan evaluasi dan rekomendasi tindak lanjut.

2 Kemitraan yang Diinisiasi oleh Mitra Eksternal

Pada kondisi tertentu, inisiatif kolaborasi berasal dari pihak eksternal. Sekolah tetap perlu memastikan bahwa program tersebut sesuai kebutuhan, aman bagi murid, dan tidak mengandung unsur promosi produk.

Tahapan	Deskripsi Kegiatan	Pihak yang Terlibat	Keluaran yang Diharapkan
1. Penawaran Program oleh Mitra	Mitra eksternal menawarkan pelatihan, pendampingan, modul, atau program edukasi lainnya.	Mitra eksternal	Proposal atau surat penawaran kerja sama.
2. Verifikasi dan Penilaian Awal	Sekolah menilai reputasi mitra, kesesuaian materi, dan memastikan kegiatan bebas dari promosi.	Kepala sekolah, tim kurikulum, komite sekolah	Hasil penilaian kelayakan program.

Tahapan	Deskripsi Kegiatan	Pihak yang Terlibat	Keluaran yang Diharapkan
3. Konsultasi dan Penyesuaian Materi	Sekolah mengusulkan penyesuaian agar materi sesuai konteks sekolah dan usia murid.	Sekolah dan mitra	Materi pembelajaran yang telah disesuaikan.
4. Kesepakatan dan Persiapan Teknis	Penyusunan MoU atau perjanjian kerja sama yang berisi pembagian peran, waktu, dan tanggung jawab.	Sekolah dan mitra	Dokumen kesepakatan dan jadwal kegiatan.
5. Pelaksanaan Program Edukasi	Program dilaksanakan di sekolah dengan fasilitasi dari mitra dan dukungan penuh pihak sekolah.	Sekolah dan mitra	Pembelajaran keamanan siber yang aplikatif.
6. Evaluasi Bersama dan Pelaporan	Evaluasi dilakukan untuk menilai efektivitas program dan peluang kolaborasi berkelanjutan.	Sekolah dan mitra	Laporan kegiatan dan rekomendasi lanjutan.

A Tip untuk Sekolah Non-3T

Sekolah non-3T umumnya memiliki akses yang lebih memadai terhadap jaringan internet, perangkat digital, guru TIK, serta jejaring mitra seperti perguruan tinggi, industri, atau komunitas digital. Kondisi ini memungkinkan bentuk kolaborasi yang lebih variatif dan berorientasi pada penguatan kompetensi teknis maupun pengembangan ekosistem digital sekolah.

Tip 1 Manfaatkan Akses Teknologi untuk Program Pembelajaran Lanjutan

Gunakan infrastruktur digital yang sudah tersedia untuk menjalin kolaborasi dengan akademisi dalam mengembangkan kurikulum keamanan siber, modul tematik, atau bahan ajar terpadu.

Tip 2 Gandeng Industri untuk Pelatihan Teknis Intensif

Ajak industri teknologi untuk memberikan pelatihan teknis tingkat lanjut, seperti pengenalan ancaman siber, pengelolaan akun digital, atau simulasi insiden siber dalam skala sederhana.

Tip 3 Kembangkan Laboratorium Mini Keamanan Siber

Bagi sekolah yang memiliki dukungan perangkat, buat laboratorium mini sebagai ruang praktik murid dan guru, baik untuk latihan dasar maupun untuk program ekstrakurikuler seperti klub siber.

Tip 4 Jadwalkan Kelas Inspirasi dan *Mentoring* Jangka Panjang

Kolaborasi dengan akademisi dan industri dapat diperluas melalui kelas inspirasi, sesi berbagi pengalaman, atau mentoring berkala yang memberi wawasan karier digital bagi murid.

Tip 5 Optimalkan Webinar Rutin

Ketersediaan internet stabil memungkinkan sekolah untuk mengadakan webinar rutin dengan pakar keamanan siber, sehingga guru dan murid dapat terus memperbarui literasi digitalnya.

B Tip untuk Sekolah 3T

Sekolah yang berada di wilayah 3T memiliki tantangan yang lebih kompleks, seperti keterbatasan akses internet, perangkat digital, dan tenaga pendidik TIK. Oleh karena itu, pendekatan kemitraan perlu bersifat adaptif, realistis, dan berorientasi keberlanjutan jangka panjang, bukan hanya kegiatan sekali datang.

Tip 1 Prioritaskan Materi Pembelajaran yang Dapat Diakses Secara Offline

Dorong mitra untuk menyediakan modul cetak, video offline, atau USB berisi materi agar pembelajaran tidak bergantung pada internet. Materi harus sederhana, kontekstual, dan mudah diimplementasikan guru di kelas.

Tip 2 Libatkan Komunitas Lokal sebagai Pendamping Guru

Kemitraan dapat diperkuat melalui relawan TIK lokal, penyuluh digital desa, atau komunitas literasi digital yang dapat hadir secara langsung dan lebih rutin mendampingi guru.

Tip 3 **Perkuat Kemitraan dengan Pemerintah Daerah**

Melibatkan dinas pendidikan, perangkat desa, lembaga bantuan hukum, atau paralegal komunitas membantu memperkaya edukasi tentang hak digital, etika siber, serta perlindungan data pribadi dengan pendekatan yang relevan bagi murid di wilayah 3T.

Tip 4 **Manfaatkan Program Pelatihan Bergerak (*Mobile Training Unit*)**

Jika akses geografis sulit, mitra dapat mengadakan pelatihan lapangan menggunakan kendaraan operasional yang dilengkapi perangkat. Pendekatan ini memungkinkan murid dan guru belajar tanpa perlu berpindah lokasi jauh.

Tip 5 **Gunakan Pendekatan Klaster Wilayah untuk Efisiensi**

Untuk menekan biaya dan meningkatkan efektivitas, satu program kemitraan dapat dirancang untuk beberapa sekolah dalam satu kecamatan. Skema klaster memudahkan koordinasi, berbagi fasilitas, dan memperluas dampak.

E Evaluasi Kemitraan Pendidikan Keamanan Siber

Evaluasi merupakan bagian yang tidak terpisahkan dari pelaksanaan kemitraan pendidikan keamanan siber. Evaluasi diperlukan untuk memastikan bahwa bentuk dukungan, kegiatan, dan hasil program selaras dengan kebutuhan sekolah serta memberikan dampak nyata bagi murid dan pendidik. Melalui evaluasi, sekolah dapat menilai efektivitas pelaksanaan kegiatan, memantau ketercapaian tujuan, mengidentifikasi kendala, dan merumuskan rencana perbaikan maupun keberlanjutan program.

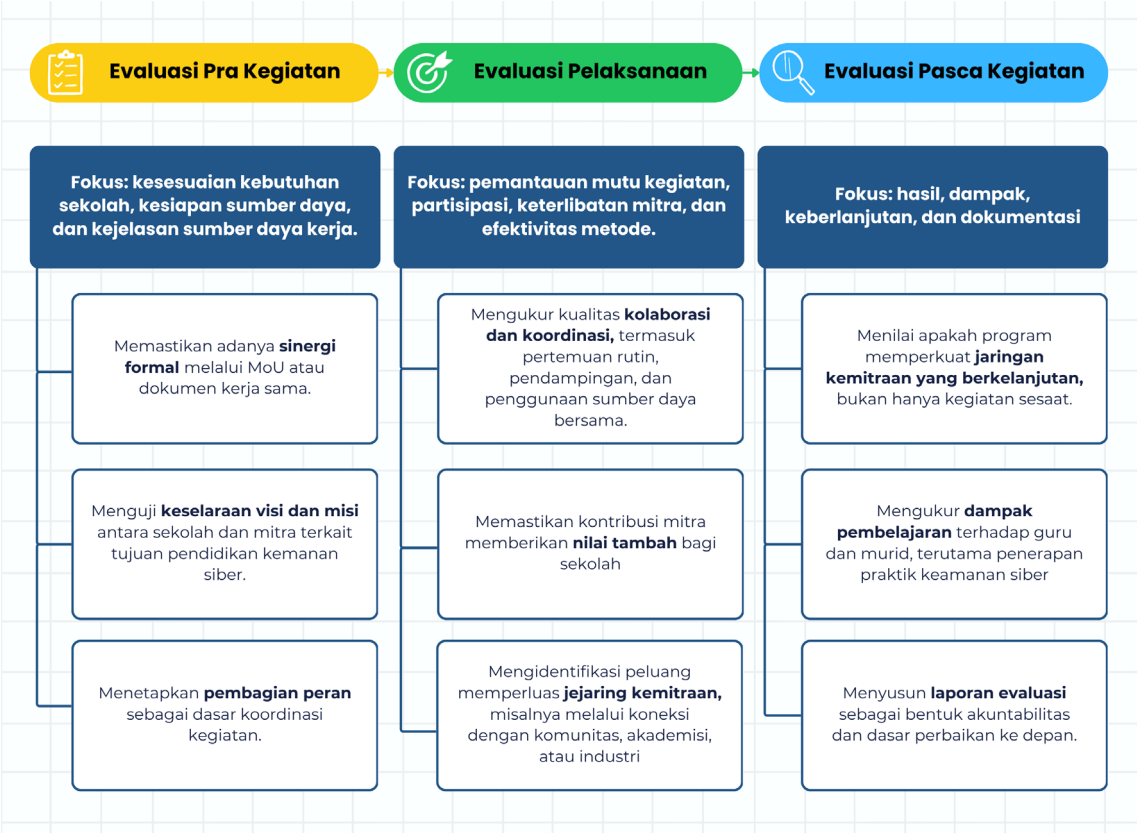
Evaluasi kemitraan dilakukan secara kolaboratif oleh berbagai pihak di lingkungan sekolah dan mitra eksternal. **Kepala sekolah** berperan sebagai penanggung jawab utama yang memastikan proses evaluasi berjalan sesuai prinsip akuntabilitas. **Tim kurikulum atau tim penggerak kemitraan** bertugas mengoperasikan instrumen evaluasi, mengumpulkan data, serta menyusun analisis awal. **Pendidik atau fasilitator internal** memberikan penilaian terhadap kualitas materi, metode, serta keterlibatan murid selama program berlangsung.

Di sisi lain, **mitra eksternal** baik dari pemerintah, komunitas, akademisi, maupun industri dapat berkontribusi pada penilaian relevansi, mutu pelaksanaan, serta dampak kegiatan.

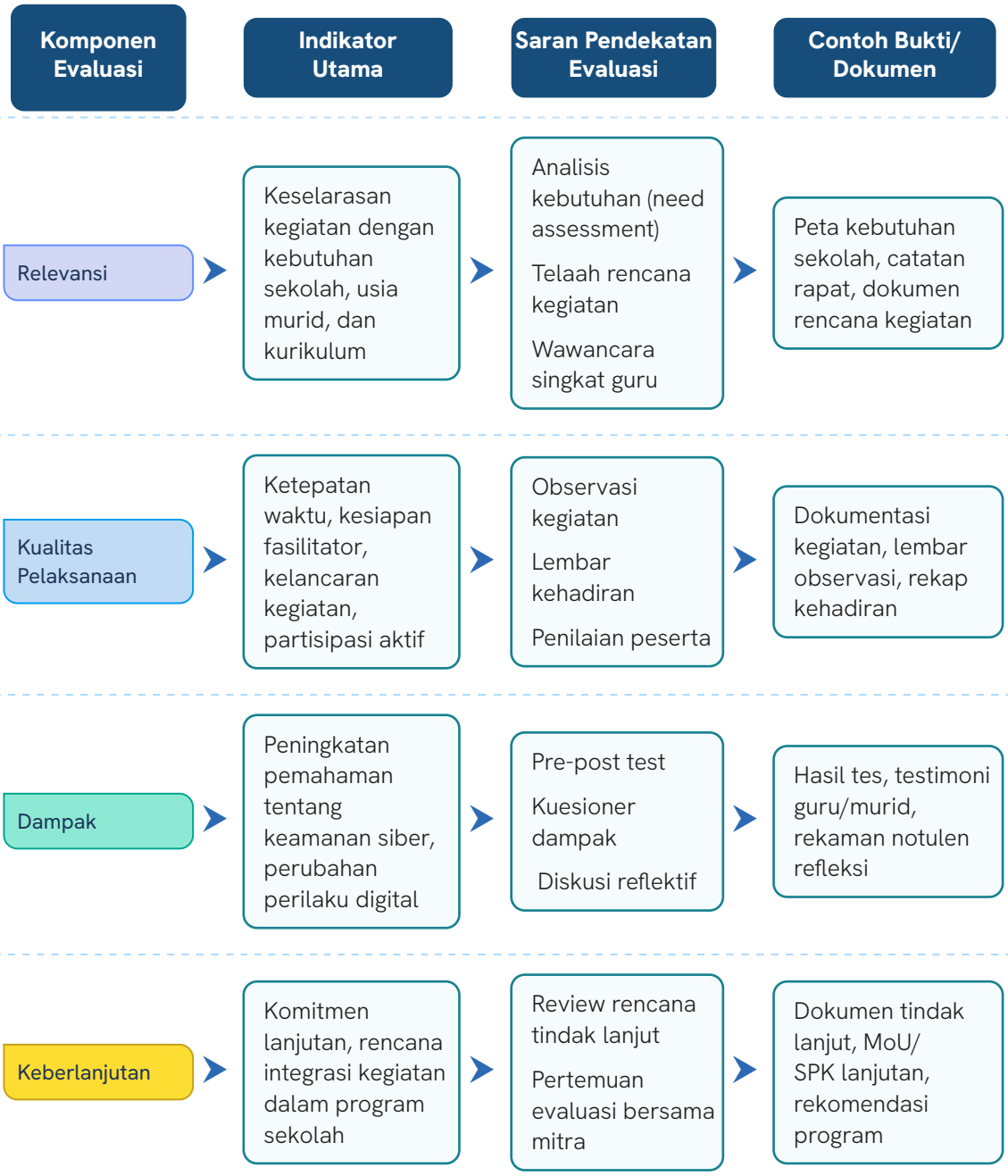
Apabila diperlukan, **komite sekolah** juga dapat memberikan masukan tambahan, terutama terkait relevansi program terhadap kebutuhan komunitas belajar.

Pelaksanaan evaluasi pada tahap pra-kegiatan, pelaksanaan, dan pasca-kegiatan tidak bersifat wajib untuk dilakukan secara lengkap. Setiap satuan pendidikan dapat menyesuaikan kedalaman dan cakupan evaluasi berdasarkan kapasitas sumber daya, kesiapan instrumen, serta tingkat dukungan dari mitra.

Meskipun demikian, **evaluasi pasca-kegiatan merupakan tahap minimum** yang perlu dilaksanakan oleh setiap sekolah. Evaluasi pasca menyediakan gambaran menyeluruh mengenai hasil, dampak, dan keberlanjutan program, sehingga menjadi dasar penting untuk peningkatan kualitas kemitraan dan pemenuhan prinsip akuntabilitas



Tabel berikut dapat digunakan sebagai **indikator umum** dan **saran pendekatan evaluasi**. Indikator ini bersifat fleksibel namun disarankan sebagai standar minimal untuk menjaga konsistensi data.



Evaluasi kemitraan tidak bersifat kaku. Meskipun indikator dan pendekatan di atas dapat digunakan sebagai standar, **metode evaluasi tetap harus disesuaikan dengan konteks kegiatan, kapasitas sekolah, dan bentuk dukungan mitra**. Setiap sekolah dapat menambahkan instrumen lain yang dianggap relevan selama tetap mengacu pada prinsip akuntabilitas, objektivitas, dan keberlanjutan.

Dengan evaluasi yang terencana dan terstandar, sekolah dapat memastikan bahwa kemitraan pendidikan keamanan siber benar-benar memberikan manfaat, memperkuat budaya aman digital, dan mendukung pembelajaran yang berkelanjutan

Lampiran

Lampiran 1 Peta Kompetensi Pendidikan Keamanan Siber dan Rekomendasi Aktivitas

Peta Kompetensi Pendidikan Keamanan Siber

Elemen	Deskripsi Elemen	PAUD	SD	SMP	SMA
1. **Kesadaran Keamanan Siber**	Pemahaman terhadap ancaman dan risiko siber, serta membangun pola pikir dan kebiasaan untuk melindungi diri di ruang siber.	Murid memahami bahwa penggunaan perangkat teknologi harus dengan pendampingan orang tua/wali atau pendidik	Murid mengidentifikasi aplikasi dan konten di ruang siber sesuai usia	Murid dapat mengelola waktu penggunaan perangkat teknologi digital	Murid dapat mengatur penggunaan media sosial dan internet secara produktif dan sehat
			Murid mengikuti aturan penggunaan perangkat digital dan internet	Murid dapat mengidentifikasi jenis-jenis ancaman siber	Murid dapat mengidentifikasi dan mencegah risiko siber
				Murid dapat mengidentifikasi permintaan informasi pribadi pada penggunaan aplikasi atau platform daring	Murid dapat menganalisis risiko pembuatan akun pada platform digital

Elemen	Deskripsi Elemen	PAUD	SD	SMP	SMA
2. Pelindungan Data Pribadi & Jejak Digital	Pemahaman terhadap jenis-jenis data pribadi, mengelola informasi yang dibagikan, serta menyadari bahwa setiap aktivitas di ruang siber meninggalkan jejak yang memiliki konsekuensi.	Murid dapat mengidentifikasi informasi pribadi dasar	Murid memahami pengelolaan data pribadi dan batasan berbagi informasi	Murid memahami risiko membagikan informasi pribadi di ruang siber	Murid memahami hak dan tanggungjawab atas data pribadi pihak lain yang sedang ia pegang
			Murid memahami konsekuensi jejak digital	Murid dapat menganalisis dampak jejak digital terhadap reputasi pribadi	Murid dapat memahami prinsip manajemen identitas daring
3. Etika & Perilaku Digital	Kemampuan berinteraksi secara bertanggung jawab di ruang siber, antara lain dengan bersikap sopan, menghargai hak orang lain, dan menolak perilaku merugikan seperti penyebaran informasi tidak benar atau perundungan daring.	Murid mengetahui perilaku aman saat menggunakan perangkat teknologi	Murid memahami berbagai bentuk perilaku merugikan di ruang siber	Murid menunjukkan perilaku etis dalam berinteraksi di ruag siber untuk membangun ekosistem yang aman dan sehat	Murid dapat menerapkan langkah-langkah menjaga citra positif
		Murid mengetahui perilaku aman saat berkomunikasi secara daring	Murid memahami perilaku yang menghormati privasi	Murid memahami konsep persetujuan (consent) di ruang siber	Murid dapat mengevaluasi perilaku di ruang siber sesuai etika digital

Elemen	Deskripsi Elemen	PAUD	SD	SMP	SMA
			Murid memahami perundungan siber dan tahu cara melapor	Murid dapat menjelaskan bentuk dan dampak perundungan siber serta dapat mempraktikkan langkah pelindungan untuk melindungi diri dan orang lain	Murid dapat menerapkan langkah-langkah pencegahan dan penanganan perundungan siber
			Murid memahami bahwa membagikan informasi yang belum pasti kebenarannya bisa merugikan orang lain	Murid dapat menganalisis dampak sosial penyebaran konten negatif dan berperan aktif melakukan pencegahan	Murid dapat mengidentifikasi konflik digital dan memilih interaksi yang aman
					Murid dapat memproduksi dan menyebarkan konten perilaku positif

Elemen	Deskripsi Elemen	PAUD	SD	SMP	SMA
4. Keterampilan Teknis Keamanan Siber	Kemampuan menerapkan perilaku aman di ruang siber dan pemahaman terhadap konsep dasar kriptografi serta penerapannya dalam mengamankan perangkat, akun, dan data.	Murid dapat menolak permintaan informasi pribadi	Murid dapat mengkomunikasikan situasi yang tidak aman di ruang siber kepada orang tua/wali atau pendidik	Murid dapat menyusun laporan kejahatan siber serta melaporkan kepada orang tua/wali atau pendidik	Murid dapat menyampaikan laporan insiden siber.
			Murid dapat menerapkan pengamanan pada perangkat teknologi	Murid dapat menerapkan pengaturan keamanan dan privasi pada perangkat dan akun digital yang digunakan di bawah bimbingan orang tua/wali	Murid dapat menerapkan dan menilai langkah pengamanan perangkat dan akun.
			Murid dapat mengidentifikasi ciri-ciri informasi yang meragukan	Murid menerapkan verifikasi kebenaran informasi	Murid dapat embedakan opini, fakta, dan propaganda.
			Murid memahami penggunaan kata sandi	Murid memahami peran kriptografi dalam kehidupan sehari-hari	Murid dapat menerapkan teknik enkripsi dasar.

Elemen	Deskripsi Elemen	PAUD	SD	SMP	SMA
5. Kesadaran Hukum di Ruang Siber	Pemahaman terhadap peraturan perundang-undangan terkait ruang siber, antara lain informasi dan transaksi elektronik, hak cipta, privasi, dan pelindungan data.		Murid mengetahui aturan dasar terkait ruang siber	Murid mengetahui aturan hukum dasar terkait aktivitas daring remaja	Murid dapat menjelaskan hubungan regulasi siber, hak digital, dan kewajiban hukum.
				Murid memahami keterkaitan antara perilaku daring yang aman dan kepatuhan hukum	Murid dapat menganalisis pelanggaran siber dan jenis-jenisnya.

Rekomendasi Aktivitas dalam Implementasi Pendidikan Keamanan Siber

Jenjang PAUD

Elemen	Deskripsi Elemen	Kompetensi	Rekomendasi Aktivitas
1. **Kesadaran Keamanan Siber**	Pemahaman terhadap ancaman dan risiko siber, serta membangun pola pikir dan kebiasaan untuk melindungi diri di ruang siber.	Murid memahami bahwa penggunaan perangkat teknologi harus dengan pendampingan orang tua/ wali atau pendidik	▪ Meminta izin sebelum menggunakan perangkat teknologi ▪ Mengenali siapa orang yang perlu mendampingi saat menggunakan perangkat teknologi ▪ Mengenal konsep "Kalau takut → berhenti → panggil orang dewasa." ▪ "Kalau bingung → jangan disentuh → cari pendamping." ▪ Menerima pengawasan orang tua/ wali atau pendidikan sebagai bentuk perlindungan
2. **Pelindungan Data Pribadi & Jejak Digital**	Pemahaman terhadap jenis-jenis data pribadi, mengelola informasi yang dibagikan, serta menyadari bahwa setiap aktivitas di ruang siber meninggalkan jejak yang memiliki konsekuensi.	Murid mengidentifikasi informasi pribadi dasar	▪ Mengidentifikasi data pribadi dasar (nama, alamat, foto, video pribadi) ▪ Mempelajari bahwa "tidak semua orang di internet adalah teman"

Elemen	Deskripsi Elemen	Kompetensi	Rekomendasi Aktivitas
3. **Etika & Perilaku Digital**	Kemampuan berinteraksi secara bertanggung jawab di ruang siber, antara lain dengan bersikap sopan, menghargai hak orang lain, dan menolak perilaku merugikan seperti penyebaran informasi tidak benar atau perundungan daring.	Murid mengetahui perilaku aman saat menggunakan perangkat teknologi	▪ Tidak membagikan foto ▪ Tidak merespons pesan dari orang asing ▪ Meminta bantuan saat bingung
		Murid mengetahui perilaku aman saat berkomunikasi secara daring	▪ Menggunakan bahasa sopan saat berkomunikasi secara daring, bisa disertai dengan permainan "sopan atau tidak sopan"
4. **Keterampilan Teknis Keamanan Siber**	Kemampuan menerapkan perilaku aman di ruang siber dan pemahaman terhadap konsep dasar kriptografi serta penerapannya dalam mengamankan perangkat, akun, dan data.	Murid dapat menolak permintaan informasi pribadi	▪ Mengatakan "tidak" dengan percaya diri ▪ Melaporkan jika ada yang meminta informasi pribadi atau foto ▪ Mengidentifikasi dan membedakan rasa nyaman vs tidak nyaman

Jenjang SD

Elemen	Deskripsi Elemen	Kompetensi	Rekomendasi Aktivitas
1. **Kesadaran Keamanan Siber**	Pemahaman terhadap ancaman dan risiko siber, serta membangun pola pikir dan kebiasaan untuk melindungi diri di ruang siber.	Murid mengidentifikasi aplikasi dan konten di ruang siber sesuai usia	▪ Mengecek ikon rating usia pada aplikasi ▪ Memilih aplikasi edukatif ▪ Mengenali konten tidak sesuai usia

Elemen	Deskripsi Elemen	Kompetensi	Rekomendasi Aktivitas
		Murid mengikuti aturan penggunaan perangkat digital dan internet	▪ Menjalankan jadwal screen time, mematuhi aturan sekolah, berhenti bermain saat waktu habis, bekerjasama dengan orang tua melalui formulir kesepakatan screen time di rumah.
2. **Pelindungan Data Pribadi & Jejak Digital**	Pemahaman terhadap jenis-jenis data pribadi, mengelola informasi yang dibagikan, serta menyadari bahwa setiap aktivitas di ruang siber meninggalkan jejak yang memiliki konsekuensi.	Murid memahami pengelolaan data pribadi dan batasan berbagi informasi	▪ Mengenali informasi yang boleh dibagikan dan tidak ▪ Mengatur siapa saja yang boleh diberitahu soal data pribadi ▪ Mengenali modus-modus permintaan data pribadi yang tidak boleh dibagikan
		Murid memahami konsekuensi jejak digital	▪ Mengelompokan contoh unggahan ke dalam kategori positif atau negatif ▪ Mengetahui konsekuensi dari unggahan di media sosial, dapat disertai dengan latihan untuk menilai unggahan
3. **Etika & Perilaku Digital**	Kemampuan berinteraksi secara bertanggung jawab di ruang siber, antara lain dengan bersikap sopan, menghargai hak orang lain, dan menolak perilaku merugikan seperti penyebaran informasi tidak benar atau perundungan daring.	Murid memahami berbagai bentuk perilaku merugikan di ruang siber	▪ Mengidentifikasi contoh komentar kasar, ejekan, video negatif, sebagai bentuk perilaku negatif di ruang siber, dapat disertai latihan membedakan sopan atau tidak sopan

Elemen	Deskripsi Elemen	Kompetensi	Rekomendasi Aktivitas
		Murid memahami perilaku yang menghormati privasi	▪ Bermain peran (*role play*) meminta izin kepada orang lain sebelum mengambil foto/ video (Kalimat pertanyaan sederhana) ▪ Mengelompokan contoh situasi kedalam kategori yang boleh dibagikan atau tidak boleh dibagikan
		Murid memahami bahwa membagikan informasi yang belum pasti kebenarannya bisa merugikan orang lain	▪ Mengenali dampak penyebaran informasi palsu
		Murid memahami perundungan siber dan tahu cara melapor	▪ Mengenali bentuk perundungan (ejekan, publikasi foto tanpa izin), latihan berkata “stop”, dan tahu cara melapor ke guru
4. Keterampilan Teknis Keamanan Siber	Kemampuan menerapkan perilaku aman di ruang siber dan pemahaman terhadap konsep dasar kriptografi serta penerapannya dalam mengamankan perangkat, akun, dan data.	Murid dapat mengkomunikasikan situasi yang tidak aman di ruang siber kepada orang tua/wali atau pendidik	▪ Mengenali cara melapor jika menerima pesan mencurigakan ▪ Mengetahui cara melakukan tangkapan layar, disertai latihan menyampaikan laporan secara lisan kepada orang tua/wali/guru

Elemen	Deskripsi Elemen	Kompetensi	Rekomendasi Aktivitas
		Murid dapat menerapkan pengamanan pada perangkat teknologi	▪ Mengaktifkan PIN/POLA pada gawai ▪ - Mengatur privasi dasar dengan pendampingan
		Murid dapat mengidentifikasi ciri-ciri informasi yang meragukan	▪ Mengenalkan contoh judul berita yang berlebihan ▪ Latihan mengidentifikasi kebenaran sumber informasi
		Murid memahami penggunaan kata sandi	▪ Mengetahui fungsi sandi ▪ Membuat kata sandi dengan sederhana ▪ Bermain *caesar chiper*
5. Kesadaran Hukum di Ruang Siber	Pemahaman terhadap peraturan perundang-undangan terkait ruang siber, antara lain informasi dan transaksi elektronik, hak cipta, privasi, dan pelindungan data.	Murid mengetahui aturan dasar terkait ruang siber	▪ Mengenal bahwa setiap gambar/tulisan di internet ada pemiliknya ▪ Mengenal ketentuan penggunaan aplikasi sesuai umur ▪ Mengenal aturan penyebaran informasi pribadi (identitas, foto, video)

Jenjang SMP

Elemen	Deskripsi Elemen	Kompetensi	Rekomendasi Aktivitas
1. Kesadaran Keamanan Siber	Pemahaman terhadap ancaman dan risiko siber, serta membangun pola pikir dan kebiasaan untuk melindungi diri di ruang siber.	Murid dapat mengelola waktu penggunaan perangkat teknologi digital	▪ Mengatur fitur pembatas waktu layar (*screen time*) pada perangkat gawai ▪ membuat jadwal penggunaan gawai (seperti menuliskan jurnal perbandingan kualitas tidur/ belajar/hubungan sosial tanpa gawai vs dengan gawai)
		Murid dapat mengidentifikasi jenis-jenis ancaman siber	▪ Mengelompokkan studi kasus ke dalam 5 kategori risiko yang relevan bagi anak ▪ Menemukan ciri pesan penipuan di dalam teks contoh ▪ Mencari perbedaan antara tautan berbahaya dan tautan aman
		Murid dapat mengidentifikasi permintaan informasi pribadi pada penggunaan aplikasi atau platform daring	▪ Menyimak syarat dan ketentuan *install* aplikasi dan identifikasi informasi pribadi yang diminta ▪ Mengecek izin aplikasi
2. Pelindungan Data Pribadi & Jejak Digital	Pemahaman terhadap jenis-jenis data pribadi, mengelola informasi yang dibagikan, serta menyadari bahwa setiap aktivitas di ruang siber meninggalkan jejak yang memiliki konsekuensi.	Murid memahami risiko membagikan informasi pribadi di ruang siber	▪ Merinci/Menjelaskan/Memaparkan dampak negatif dari foto yang disalahgunakan ▪ Mengumpulkan kasus kebocoran data, dan latihan menentukan informasi aman atau tidak untuk diunggah

Elemen	Deskripsi Elemen	Kompetensi	Rekomendasi Aktivitas
		Murid dapat menganalisis dampak jejak digital terhadap reputasi pribadi	▪ Mengamati contoh profil daring baik dan buruk dan kaitannya dengan jejak digital ▪ Menilai unggahan positif atau negatif ▪ Melakukan simulasi jejak digital (Mencari jejak diri sendiri di media sosial atau mesin pencari)
3. Etika & Perilaku Digital	Kemampuan berinteraksi secara bertanggung jawab di ruang siber, antara lain dengan bersikap sopan, menghargai hak orang lain, dan menolak perilaku merugikan seperti penyebaran informasi tidak benar atau perundungan daring.	Murid menunjukkan perilaku etis dalam berinteraksi di ruang siber untuk membangun ekosistem yang aman dan sehat	▪ Mengenalkan prinsip sopan santun di ruang siber ▪ Latihan menggunakan bahasa yang sopan saat mengirim pesan/berinteraksi di ruang siber ▪ Mengisi lembar checklist klasifikasi perilaku etis dari contoh kasus yang diberikan (misalnya berita yang boleh disebarkan, berhenti menyebarkan) ▪ Memberikan apresiasi karya/postingan teman di media sosial
		Murid memahami konsep persetujuan (*consent*) di ruang siber	▪ Mempraktikkan meminta izin sebelum memotret atau mengunggah foto teman ▪ Latihan membedakan situasi yang perlu izin dan yang tidak ▪ Menghormati penolakan saat teman tidak ingin fotonya dibagikan.

Elemen	Deskripsi Elemen	Kompetensi	Rekomendasi Aktivitas
		Murid dapat menganalisis dampak sosial penyebaran konten negatif dan berperan aktif melakukan pencegahan	▪ Mengidentifikasi contoh hoaks yang sering muncul ▪ Mengidentifikasi bagaimana hoaks bisa membuat orang takut, marah, atau salah paham ▪ Bermain peran, misalnya mengajak untuk tidak membagikan konten yang merugikan.
		Murid dapat menjelaskan bentuk dan dampak perundungan siber serta dapat mempraktikkan langkah pelindungan untuk melindungi diri dan orang lain	▪ Mengidentifikasi bentuk perundungan (mengejek, mengancam, menyebar foto tanpa izin) ▪ Latihan menekan tombol blokir dan lapor pada platform ▪ Bermain peran (*role-play*) cara meminta bantuan guru/orang tua.
4. Keterampilan Teknis Keamanan Siber	Kemampuan menerapkan perilaku aman di ruang siber dan pemahaman terhadap konsep dasar kriptografi serta penerapannya dalam mengamankan perangkat, akun, dan data.	Murid dapat menyusun laporan kejahatan siber serta melaporkan kepada orang tua/wali atau pendidik	▪ Mengenalkan hal-hal yang perlu dilakukan dalam melaporkan kejahatan siber(mencatat waktu dan tempat kejadian, mengumpulkan bukti berupa tangkapan layar, mengisi formulir laporan sederhana yang disiapkan guru dan cara melapor pada guru atau orang tua.)
		Murid dapat menerapkan pengaturan keamanan dan privasi pada perangkat dan akun digital yang digunakan di bawah bimbingan orang tua/wali	▪ Mengenalkan cara mengatur izin aplikasi (kamera, mikrofon, lokasi). ▪ Mempraktikan mematikan akses aplikasi yang tidak penting ▪ Mempraktikkan meninjau pengaturan privasi default di platform yang digunakan.

Elemen	Deskripsi Elemen	Kompetensi	Rekomendasi Aktivitas
		Murid menerapkan verifikasi kebenaran informasi	▪ Melakukan validasi silang dengan membandingkan kebenaran informasi dari berbagai sumber ▪ Memeriksa kredibilitas data teknis konten (penulis, tanggal, sumber asli) ▪ menggunakan alat periksa fakta pemula yang disediakan guru.
		Murid memahami peran kriptografi dalam kehidupan sehari-hari	▪ Mengenalkan ikon gembok pada peramban sebagai tanda koneksi aman ▪ melihat contoh aplikasi pesan yang menggunakan enkripsi ▪ latihan sederhana mengirim pesan “kode” menggunakan penggantian huruf.
5. Kesadaran Hukum di Ruang Siber	Pemahaman terhadap peraturan perundang-undangan terkait ruang siber, antara lain informasi dan transaksi elektronik, hak cipta, privasi, dan pelindungan data.	Murid mengetahui aturan hukum dasar terkait aktivitas daring remaja	▪ Mengenalkan Hak Kekayaan Intelektual ▪ Studi kasus pelanggaran karya orang lain Mengenalkan data yang boleh disebarkan dan tidak boleh disebarkan ▪ Mendiskusikan contoh larangan penggunaan teknologi secara merugikan.
		Murid memahami keterkaitan antara perilaku daring yang aman dan kepatuhan hukum	▪ Mendiskusikan contoh pelanggaran ringan (misal: membocorkan kata sandi teman) ▪ Mendiskusikan contoh pelanggaran berat (misal: penyebaran foto tanpa izin)

Jenjang SMA/SMK

Elemen	Deskripsi Elemen	Kompetensi	Rekomendasi Aktivitas
1. **Kesadaran Keamanan Siber**	Pemahaman terhadap ancaman dan risiko siber, serta membangun pola pikir dan kebiasaan untuk melindungi diri di ruang siber.	Murid dapat mengatur penggunaan media sosial dan internet secara produktif dan sehat.	▪ Membatasi penggunaan aplikasi yang tidak produktif berdasarkan hasil audit yang telah dilakukan ▪ Mencocokan screen time mingguan dengan waktu belajar
		Murid dapat mengidentifikasi dan mencegah risiko siber.	▪ Mengidentifikasi modus dari berbagai jenis ancaman (penipuan, peretasan, tautan berbahaya) ▪ Mendeteksi trik manipulasi psikologis di balik pesan digital yang mencurigakan ▪ Menyusun strategi pencegahan sederhana dari contoh kasus keamanan siber
		Murid dapat menganalisis risiko pembuatan akun pada platform digital.	▪ Membandingkan izin akses dan cakupan data pribadi yang dikumpulkan oleh dua platform digital dengan fungsi serupa ▪ Menilai kewajaran antara data pribadi yang diminta dengan fungsi layanan yang ditawarkan ▪ Melakukan pemetaan risiko terhadap izin aplikasi yang diminta dan menonaktifkan yang tidak relevan dengan aplikasi

Elemen	Deskripsi Elemen	Kompetensi	Rekomendasi Aktivitas
2. Pelindungan Data Pribadi & Jejak Digital	Pemahaman terhadap jenis-jenis data pribadi, mengelola informasi yang dibagikan, serta menyadari bahwa setiap aktivitas di ruang siber meninggalkan jejak yang memiliki konsekuensi.	Murid memahami hak dan tanggungjawab atas data pribadi pihak lain yang sedang ia pegang	▪ Menyusun panduan sederhana tentang tata kelola pengumpulan data ▪ Mempraktikkan pengamanan berkas bersama ▪ latihan membuat keputusan "boleh/tidak boleh dibagikan".
		Murid dapat memahami prinsip manajemen identitas daring	▪ Memilah unggahan lama, serta menghapus atau melaporkan konten yang merugikan. ▪ Mengenalkan terkait dengan manajemen identitas daring ▪ Menyesuaikan visibilitas profil sesuai dengan kebutuhan.
		Murid dapat menerapkan langkah-langkah menjaga citra positif	▪ Mengenali kekuatan, minat, dan nilai diri ▪ Membuat profil online yang menggambarkan karakter positif(Bio yang relevan, portofolio karya, aktivitas sosial/organisasi).
3. Etika & Perilaku Digital	Kemampuan berinteraksi secara bertanggung jawab di ruang siber, antara lain dengan bersikap sopan, menghargai hak orang lain, dan menolak perilaku merugikan seperti penyebaran informasi tidak benar atau perundungan daring.	Murid dapat mengevaluasi perilaku di ruang siber sesuai etika digital.	▪ Membedah batasan antara berpendapat dengan perundungan Menulis jurnal refleksi mengenai dampak positif/negatif yang berdampak pada diri sendiri/orang lain atas unggahan yang dilakukan

Elemen	Deskripsi Elemen	Kompetensi	Rekomendasi Aktivitas
		Murid dapat mengidentifikasi konflik digital dan memilih interaksi yang aman.	▪ Menentukan kalimat provokatif atau yang dapat memicu konflik dari contoh yang diberikan ▪ Mengidentifikasi strategi meredakan konflik ▪ Mengenalkan cara menolak provokasi serta latihan memilih respons aman.
		Murid dapat memproduksi dan menyebarkan konten perilaku positif.	▪ Membuat poster digital ▪ Membuat video pendek tentang etika digital ▪ Merancang rencana unggahan
		Murid dapat menerapkan langkah-langkah pencegahan dan penanganan perundungan siber.	▪ Memahami aspek etika dan hukum dari perundungan siber ▪ Melakukan simulasi pelaporan menggunakan fitur keamanan platform ▪ Menyusun langkah perlindungan diri untuk mencegah perundungan
4. Keterampilan Teknis Keamanan Siber	Kemampuan menerapkan perilaku aman di ruang siber dan pemahaman terhadap konsep dasar kriptografi serta penerapannya dalam mengamankan perangkat, akun, dan data.	Murid dapat menyampaikan laporan insiden siber.	▪ Menyusun kerangka laporan insiden seperti (Kronologi, bukti, pihak terlibat) Menyiapkan bukti pendukung untuk pelaporan ▪ Menulis draft laporan insiden siber sesuai skenario dan otoritas yang berwenang ▪ Mensimulasikan prosedur pengiriman laporan. latihan membuat laporan berdasarkan skenario kasus.
		Murid dapat menerapkan dan menilai langkah pengamanan perangkat dan akun.	▪ Membuat kata sandi kuat ▪ Mengaktifkan verifikasi dua langkah

Elemen	Deskripsi Elemen	Kompetensi	Rekomendasi Aktivitas
			▪ Mengaktifkan enkripsi pada folder/data/media penyimpanan sensitif ▪ Melakukan pemeriksaan berkala tingkat keamanan perangkat / riwayat akses akun.
		Murid dapat membedakan opini, fakta, dan propaganda.	▪ Mengenali unsur-unsur manipulasi atau teknik propaganda dalam informasi ▪ Mengidentifikasi perbedaan gaya bahasa antara fakta dan opini dalam konten ▪ Mengklasifikasikan kategori informasi berdasarkan sifat dan tujuannya
		Murid dapat menerapkan teknik enkripsi dasar.	▪ Mengenal konsep pesan terenkripsi ▪ Menggunakan aplikasi pesan dengan enkripsi ▪ latihan mengenkripsi dan mendekripsi pesan sederhana.
5. Kesadaran Hukum di Ruang Siber	Pemahaman terhadap peraturan perundang-undangan terkait ruang siber, antara lain informasi dan transaksi elektronik, hak cipta, privasi, dan pelindungan data.	Murid dapat menjelaskan hubungan regulasi siber, hak digital, dan kewajiban hukum.	▪ Menyusun daftar Hak dan kewajiban di ruang siber. ▪ Menghubungkan berbagai contoh kasus pelanggaran digital dengan pasal atau aturan hukum yang relevan ▪ Mempresentasikan potongan regulasi yang disederhanakan.
		Murid dapat menganalisis pelanggaran siber dan jenis-jenisnya.	▪ Membaca contoh pelanggaran ringan dan berat ▪ Membahas sanksi pelanggaran ▪ Melakukan simulasi penilaian kasus ▪ Latihan membuat keputusan “pelanggaran atau tidak”.

Lampiran 2 Ide Integrasi Intrakurikuler

Contoh Integrasi Pendidikan Keamanan Siber Secara Intrakurikuler ke Dalam Mata Pelajaran

Ide Integrasi Jenjang PAUD

Elemen	Nilai Agama Dan Budi Pekerti
Capaian pembelajaran	Murid menghargai diri sendiri dan memiliki rasa syukur terhadap Tuhan YME sehingga dapat berpartisipasi aktif dalam menjaga kebersihan, kesehatan, dan keselamatan dirinya
Kompetensi pendidikan keamanan siber yang dipilih	Murid dapat menolak permintaan informasi pribadi
Tujuan Pembelajaran yang Sesuai (👍) dan Kurang Sesuai (🤔)	a. Murid mengenali hal-hal yang dapat mengancam keselamatan diri 🤔 b. Murid membedakan hal-hal yang mengancam dan mendukung keselamatan diri 🤔 c. Murid menerapkan tindakan yang mendukung keselamatan diri 👍 d. Murid merefleksi pentingnya menjaga keselamatan dirinya sebagai bentuk rasa syukur kepada Tuhan Yang Maha Esa 🤔
Ide integrasi	Mendongeng dengan boneka: “Berani bilang tidak!” di mana pendidik menggunakan boneka tangan yang berperan sebagai orang lain yang meminta foto murid.

Ide Integrasi Jenjang SD

Mata Pelajaran	Koding dan Kecerdasan Artifisial	Pendidikan Pancasila
Elemen	Literasi Digital	Undang-Undang Dasar Negara Republik Indonesia Tahun 1945
Capaian Pembelajaran	Memahami konsep dasar, manfaat, dan dampak teknologi digital, memahami sistem komputer tingkat pradasar, menerapkan pengamanan	Mengidentifikasi dan melaksanakan aturan di sekolah dan lingkungan tempat tinggal; mengidentifikasi dan

Mata Pelajaran	Koding dan Kecerdasan Artifisial	Pendidikan Pancasila
	informasi pribadi dalam komunikasi daring, memanfaatkan internet, dan memproduksi serta mendiseminasi konten digital dalam bentuk teks dan gambar.	menerapkan hak yang didapat dan kewajiban sebagai anggota keluarga dan sebagai warga sekolah.
Kompetensi Pendidikan Keamanan Siber Yang Dipilih	**Lintas Elemen:** ▪ Murid memahami konsekuensi jejak digital (elemen Pelindungan Data Pribadi & Jejak Digital) ▪ Murid mengetahui aturan dasar terkait ruang siber (elemen Kesadaran Hukum di Ruang Siber)	Murid mengikuti aturan penggunaan perangkat digital dan internet
Tujuan Pembelajaran yang Sesuai (👍) dan Kurang Sesuai (🤔)	a. Memahami konsep dasar teknologi digital 🤔 b. Memahami perangkat keras dan perangkat lunak komputer 🤔 **c. Memahami keamanan informasi pribadi 👍** **d. Menerapkan internet secara aman dan produktif 👍** **e. Memahami dampak teknologi digital 👍** **f. Menerapkan produksi konten digital dalam bentuk teks dan gambar 👍** **g. Menerapkan diseminasi konten digital dalam bentuk teks dan gambar 👍**	**a. Memahami aturan di sekolah dan lingkungan tempat tinggal. 👍** **b. Mengidentifikasi aturan di sekolah dan lingkungan tempat tinggal. 👍** c. Membuat aturan di sekolah dan lingkungan tempat tinggal. 🤔 **d. Menerapkan aturan-aturan di sekolah dan lingkungan tempat tinggal. 👍** e. Mengidentifikasi hak yang didapat dan kewajiban sebagai anggota keluarga dan sebagai warga sekolah. 🤔
Ide Integrasi	Siswa berperan sebagai "Agen Siber" yang bertugas membuat **poster kampanye digital** (menggunakan aplikasi sederhana seperti Canva) berisi imbauan menjaga data pribadi dan peringatan santun tentang aturan hukum di internet (misalnya: "Saring sebelum *Sharing*" atau "Stop *Bullying*"). Poster tersebut kemudian **diunggah ke galeri daring kelas** (seperti Padlet atau Google Slides bersama) di mana siswa lain wajib memberikan satu komentar	**Simulasi skenario**, di mana setiap kelompok murid mendapatkan kartu situasi yang menampilkan sebuah dilema digital (misalnya: '**Waktu bermain gim sudah habis, tetapi levelnya belum selesai. Apa yang kamu lakukan?**'). Murid tidak hanya menjawab, tetapi diminta untuk langsung memeragakan tindakan yang seharusnya mereka ambil sesuai aturan, seperti bangkit

Mata Pelajaran	Koding dan Kecerdasan Artifisial	Pendidikan Pancasila
	apresiasi, mensimulasikan cara menyebarkan dan merespons konten secara aman, legal, dan positif.	dari kursi dan mematikan gawai tersebut.

Ide Integrasi Jenjang SMP

Mata pelajaran	Matematika	Bahasa Inggris
Elemen	Aljabar	**Menulis - Mempresentasikan (*Writing - Presenting*)**
Capaian Pembelajaran	Mengenali, memprediksi dan menggeneralisasi pola dalam bentuk susunan benda dan bilangan; Menyatakan suatu situasi ke dalam bentuk aljabar; menggunakan sifat-sifat operasi (komutatif, asosiatif, dan distributif) untuk menghasilkan bentuk aljabar yang ekuivalen. Murid dapat memahami relasi dan fungsi (domain, kodomain, range) serta menyajikannya dalam bentuk diagram panah, tabel, himpunan pasangan berurutan, dan grafik; membedakan beberapa fungsi non linear dari fungsi linear secara grafik; menyelesaikan persamaan dan pertidaksamaan linear satu variabel; menyajikan, menganalisis, dan menyelesaikan masalah dengan menggunakan relasi, fungsi dan persamaan linear; serta menyelesaikan sistem persaman linear dua variabel melalui beberapa cara untuk penyelesaian masalah.	Murid mengomunikasikan gagasan dan pengalaman mereka dalam berbagai jenis teks secara tertulis atau teks multimodal tentang topik sehari-hari dan sesuai dengan minat dengan mulai menggunakan kalimat sederhana dan majemuk dengan struktur teks dan unsur kebahasaan yang tepat. Murid mengungkapkan pendapat dan mempertahankan argumen tentang suatu isu terkait topik sehari-hari atau yang sesuai dengan minat.
Kompetensi Pendidikan Keamanan Siber Yang Dipilih	Murid memahami peran kriptografi dalam kehidupan sehari-hari	Murid dapat menganalisis dampak jejak digital terhadap reputasi pribadi

Mata pelajaran	Matematika	Bahasa Inggris
Tujuan Pembelajaran yang Sesuai (👍) dan Kurang Sesuai (🤔)	▪ Mengidentifikasi, menentukan, dan memprediksi pola susunan benda dan bilangan serta menyelesaikan permasalahan yang terkait. 🤔 ▪ **Mengidentifikasi dan menentukan unsur-unsur (suku, konstanta, koefisien, dan variabel), menggunakan sifat-sifat dan operasi hitung bentuk aljabar serta memodelkan suatu permasalahan menjadi suatu bentuk aljabar dan menggunakannya untuk menyelesaikan permasalahan yang terkait.** 👍	▪ Mengungkapkan gagasan dalam berbagai jenis teks secara tertulis tentang topik sehari-hari dan sesuai dengan minat dengan mulai menggunakan kalimat sederhana dan majemuk dengan struktur teks dan unsur kebahasaan yang tepat. 🤔 ▪ Mengomunikasikan gagasan dan pengalaman dalam teks multimodal tentang topik sehari-hari dan sesuai dengan minat dengan mulai menggunakan kalimat sederhana dan majemuk dengan struktur teks dan unsur kebahasaan yang tepat. 🤔 ▪ **Mengungkapkan pendapat tentang suatu isu terkait kehidupan sehari-hari dan yang sesuai dengan minat.** 👍 ▪ **Mempertahankan pendapat tentang suatu isu terkait kehidupan sehari-hari dan yang sesuai dengan minat.** 👍
Ide Integrasi	Siswa diperkenalkan pada *Caesar Cipher* (sandi geser) dan ditantang untuk **memodelkan aturan geserannya menjadi persamaan aljabar** sederhana, misalnya $y = x + k$ (di mana y adalah posisi huruf sandi, x adalah posisi huruf asli, dan k adalah kunci geseran). Dalam proses ini, siswa harus **mengidentifikasi unsur aljabarnya**: menetapkan x dan y sebagai variabel (karena nilainya berubah-ubah) dan k sebagai **konstanta** (karena angka geserannya	**Studi kasus jejak digital**: murid mengkaji/menganalisis suatu kasus tentang jejak digital seorang tokoh media sosial (*influencer*) dan mempresentasikan hasilnya yang meliputi pendapatnya tentang dampak positif & negatif dari jejak digital terhadap reputasi *influencer* tersebut dan meluaskan konteksnya ke reputasi pribadi murid.

Mata pelajaran	Matematika	Bahasa Inggris
	tetap). Kegiatan ditutup dengan siswa menggunakan "rumus aljabar" temuan mereka untuk menyandikan (enkripsi) sebuah pesan rahasia berisi tips keamanan siber, lalu merefleksikan pentingnya enkripsi tersebut dalam kehidupan.	

Ide Integrasi Jenjang SMA

Mata Pelajaran	Koding dan Kecerdasan Artifisial	Ilmu Pengetahuan Sosial
Elemen	Literasi Digital	Pemahaman Konsep
Capaian Pembelajaran	Pada akhir Fase E, murid mampu menerapkan produksi dan diseminasi konten digital dalam bentuk sajian multimedia.	Pada akhir Fase E, murid mampu menjelaskan konsep dasar geografi, fenomena geografi fisik melalui litosfer, atmosfer, dan hidrosfer sebagai ruang hidup, serta mengimplementasikan teknologi geospasial berupa peta, penginderaan jauh dan Sistem Informasi Geografis (SIG); menelaah hakikat ilmu ekonomi sebagai ilmu yang mempelajari upaya manusia dalam memenuhi kebutuhan hidupnya; membedakan produk keuangan bank dan nonbank sebagai dasar dalam menggunakan produk dan layanan, risiko keuangan dan menyusun laporan keuangan pribadi; menjelaskan fungsi sosiologi sebagai ilmu yang secara kritis, analitis, kreatif, dan solutif mengkaji masyarakat. menelaah status dan peran individu dalam kelompok sosial dan memberikan contoh berbagai ragam gejala sosial yang ada di dalam masyarakat; menganalisis keragaman manusia dan budayanya

Mata Pelajaran	Koding dan Kecerdasan Artifisial	Ilmu Pengetahuan Sosial
		sebagai bagian dari masyarakat multikultural; menelaah konsep dasar ilmu sejarah dan mengimplementasikan penelitian sejarah untuk merefleksikan keterhubungan antara masa lampau, masa kini, dan masa yang akan datang melalui berbagai peristiwa atau kejadian penting dalam lingkup lokal, nasional dan global mulai dari masa kerajaan Hindu-Buddha hingga masa kerajaan Islam
Contoh Kompetensi Pendidikan Keamanan Siber Yang Dipilih	Murid dapat memproduksi dan menyebarkan konten perilaku positif.	Murid dapat mengidentifikasi konflik digital dan memilih interaksi yang aman.
Tujuan Pembelajaran yang Sesuai (👍) dan Kurang Sesuai (🤔)	▪ Memahami konsep dasar teknologi digital ▪ **Memahami keamanan informasi pribadi👍** ▪ **Menerapkan internet secara aman dan produktif👍** ▪ **Memahami dampak teknologi digital👍** ▪ Menerapkan produksi konten digital dalam bentuk teks dan gambar🤔	▪ Menjelaskan fungsi sosiologi sebagai ilmu secara kritis, analitis, kreatif, dan solutif mengkaji masyarakat. 🤔 ▪ **Menelaah status dan peran individu dalam kelompok sosial serta ragam gejala sosial yang ada di masyarakat.👍** ▪ Menganalisis keragaman manusia dan budayanya sebagai bagian dari masyarakat multikultural.🤔

Mata Pelajaran	Koding dan Kecerdasan Artifisial	Ilmu Pengetahuan Sosial
Ide Integrasi	Memproduksi konten untuk kampanye "saling jaga", bekerjasama dengan orang tua dan komunitas sekitar dengan tujuan mencegah perundungan di ruang siber.	Siswa melakukan analisis studi kasus terhadap fenomena sosial digital yang sedang tren (seperti *cancel culture* atau *cyberbullying* massal) untuk membedah status dan peran aktor yang terlibat (misalnya: siapa yang berperan sebagai provokator, korban, atau *bystander*). Dalam diskusi kelompok, siswa diminta mengevaluasi bagaimana anonimitas di ruang siber dapat mengubah perilaku sosial seseorang, lalu merumuskan strategi bagaimana seorang individu seharusnya menjalankan "peran"-nya secara etis untuk meredam konflik tersebut.

Ide Integrasi Jenjang SMK

Kelompok Bisnis dan Manajemen

	Akuntansi Keuangan dan Lembaga	Bisnis Digital
Mata Pelajaran	Dasar-Dasar Akuntansi dan Keuangan Lembaga (Fase E)	Dasar-Dasar Pemasaran (Fase E)
Elemen	Kecakapan kerja dasar (*basic job skills*), K3, dan budaya kerja	Wawasan dunia kerja bidang pemasaran di berbagai industri

	Akuntansi Keuangan dan Lembaga	Bisnis Digital
Capaian Pembelajaran	Menerapkan regulasi dan standar yang mengatur etika profesi akuntansi dan keuangan lembaga, kode etik dalam praktik akuntansi dan keuangan lembaga, prinsip-prinsip etika profesi akuntansi dan keuangan lembaga, praktik-praktik kesehatan diri dan keselamatan kerja, praktik budaya kerja 5R, dasar-dasar akuntansi, dasar-dasar perbankan, produk dan jasa layanan perbankan, serta penggunaan paket program pengolah angka (*spreadsheet*).	Menganalisis proses bisnis dalam bidang pemasaran secara menyeluruh pada berbagai jenis industri dan usaha, perkembangan pemasaran mulai dari konvensional sampai dengan penerapan teknologi modern, industri 4.0, *Internet of Things* (IoT), teknologi digital dalam pemasaran, isu-isu perkembangan yang muncul dan hilang ke depan terkait dengan dunia pemasaran, seperti *digital marketing, e-commerce, marketplace*, media sosial, dan sejenisnya, profil pekerjaan/profesi (*job profile*) dalam bidang pemasaran di masa sekarang dan dimasa mendatang, seperti kasir, pramuniaga, *sales executive, merchandiser, digital marketer, public relation*, dan sejenisnya, serta peluang usaha di bidang pemasaran, seperti *dropshipping, drop servicing, affiliate marketing, marketing agency, content creator,* dan sejenisnya, serta mampu menentukan karir di bidang yang sesuai dengan bakat, minat, dan renjana (*passion*).
Kompetensi Pendidikan Keamanan Siber Yang Dipilih	Murid dapat menganalisis risiko pembuatan akun pada platform digital.	Murid dapat mengidentifikasi konflik digital dan memilih interaksi yang aman.

	Akuntansi Keuangan dan Lembaga	Bisnis Digital
Tujuan Pembelajaran yang (👍) dan Kurang Sesuai (🤔)	▪ **Menerapkan regulasi dan standar yang mengatur etika profesi akuntansi dan keuangan lembaga** 👍 ▪ **Menerapkan kode etik dalam praktik akuntansi dan keuangan lembaga**□ ▪ **Menerapkan prinsip-prinsip etika profesi akuntansi dan keuangan lembaga, praktik-praktik** 👍 ▪ **Menerapkan praktik-praktik kesehatan diri dan keselamatan kerja, praktik budaya kerja 5R** 👍 ▪ Memahami dasar-dasar akuntansi, dasar-dasar perbankan, produk dan jasa layanan perbankan 🤔	▪ Menganalisis proses bisnis dalam bidang pemasaran secara menyeluruh pada berbagai jenis industri dan usaha 🤔 ▪ **Menganalisis teknologi digital dalam pemasaran,** 👍 ▪ Menganalisis isu-isu perkembangan yang muncul dan hilang ke depan terkait dengan dunia pemasaran, seperti digital marketing, e-commerce, marketplace, media sosial, dan sejenisnya, 🤔
Kompetensi Pendidikan Keamanan Siber Yang Sesuai	Murid mampu menganalisis risiko pembuatan akun di berbagai platform dan aplikasi digital berdasarkan berbagai variabel (syarat dan ketentuan, informasi atau data yang diperlukan, hak akses platform atau aplikasi, dan lain-lain)	Murid mampu mengidentifikasi potensi konflik atau kerugian pada situasi tertentu di ruang siber, serta menentukan cara berinteraksi yang aman dan menghargai semua pihak

	Akuntansi Keuangan dan Lembaga	Bisnis Digital
Ide Integrasi	Murid menganalisis risiko pembuatan akun pada platform digital yang sering digunakan dalam dunia kerja akuntansi, seperti aplikasi keuangan, marketplace, dan perbankan digital. Mereka menelaah syarat dan ketentuan layanan, jenis data keuangan atau pribadi yang diminta (misalnya nomor rekening, NPWP, atau data transaksi), serta hak akses aplikasi terhadap perangkat. Hasil analisis dituangkan dalam tabel penilaian risiko dan dibahas dalam konteks etika profesi akuntansi, keamanan data pelanggan, serta tanggung jawab menjaga kerahasiaan informasi keuangan.	Murid menganalisis berbagai kasus nyata terkait konflik di ruang siber, seperti komentar negatif pelanggan di media sosial, pencurian ide bisnis online, atau penyalahgunaan data pelanggan oleh pihak ketiga. Dalam kelompok kecil, mereka mengidentifikasi potensi konflik atau kerugian yang bisa terjadi bagi perusahaan dan konsumen, kemudian merancang strategi komunikasi digital yang etis. Misalnya menulis tanggapan profesional di media sosial, membuat kebijakan privasi sederhana, atau menyusun panduan interaksi pelanggan yang aman dan menghargai semua pihak.

Kelompok Teknologi dan Informasi

	Teknik Jaringan Komputer dan Telekomunikasi	Pengembangan Perangkat Lunak dan Gim
Mata Pelajaran	Teknik Komputer dan Jaringan (Fase F)	Dasar-Dasar Pengembangan Perangkat Lunak dan Gim (Fase E)
Elemen	Keamanan Jaringan	Wawasan dunia kerja bidang pengembangan perangkat lunak dan gim
Capaian Pembelajaran	Menerapkan sistem keamanan jaringan. (Meliputi analisis sistem keamanan jaringan yang diperlukan, potensi ancaman dan serangan terhadap keamanan	Menganalisis langkah-langkah kerja dalam pengembangan perangkat lunak dan gim dengan metode yang menerapkan prinsip sesuai kebutuhan pelanggan; menganalisis perkembangan

	Teknik Jaringan Komputer dan Telekomunikasi	Pengembangan Perangkat Lunak dan Gim
	jaringan, langkah-langkah penguatan host (host hardening), server Demilitarized Zone (DMZ), pengujian keamanan jaringan, host dan server, fungsi, cara kerja server autentikasi, sistem pendeteksi dan penahan ancaman atau serangan yang masuk ke jaringan, tata cara pengamanan komunikasi data menggunakan teknik kriptografi.)	teknologi di bidang perangkat lunak, jaringan komputer, cloud computing, dan gim; menganalisis berbagai profesi serta peluang kewirausahaan di bidang tersebut; serta menyimpulkan pentingnya personal branding untuk membangun rencana karier, mentransfer minat dan semangat ke dalam upaya berkarir atau berwirausaha di industri perangkat lunak dan gim.
Kompetensi Pendidikan Keamanan Siber yang Dipilih	Menerapkan teknik enkripsi dasar.	Murid dapat memahami prinsip manajemen identitas daring
Tujuan Pembelajaran yang (👍) dan Kurang Sesuai (🤔)	▪ **Menganalisis sistem keamanan jaringan yang diperlukan pada suatu kondisi tertentu** 👍 ▪ **Menerapkan tata cara pengamanan komunikasi data menggunakan teknik kriptografi** 👍	▪ Menganalisis langkah-langkah kerja dalam pengembangan perangkat lunak dan gim dengan metode yang menerapkan prinsip sesuai kebutuhan pelanggan. 🤔 ▪ **Menyimpulkan pentingnya personal branding untuk membangun rencana karier, mentransfer minat dan semangat ke dalam upaya berkarir atau berwirausaha di industri perangkat lunak dan gim.** 👍
Kompetensi Pendidikan Keamanan Siber yang Sesuai	Murid mampu menerapkan teknik kriptografi tertentu (misal: enkripsi pada komunikasi daring) sebagai salah satu langkah pengamanan digital	Murid mampu memahami prinsip manajemen identitas daring dan menerapkan langkah-langkah dalam menjaga citra positif di ruang siber

	Teknik Jaringan Komputer dan Telekomunikasi	Pengembangan Perangkat Lunak dan Gim
Ide Integrasi	Murid melakukan proyek mini bertema "**Pesan Rahasia di Dunia Digital**" dengan menerapkan teknik kriptografi sederhana seperti **Caesar cipher, Vigenère cipher**, atau **AES** untuk mengenkripsi dan mendekripsi pesan teks dalam komunikasi daring (misalnya melalui chat lokal atau simulasi email). Mereka membandingkan hasil pesan asli dan terenkripsi, menganalisis tingkat keamanannya, serta mendiskusikan bagaimana teknik ini digunakan dalam protokol keamanan jaringan nyata seperti HTTPS atau VPN. Hasilnya dituangkan dalam laporan singkat yang menjelaskan proses, hasil uji coba, dan refleksi pentingnya kriptografi dalam menjaga keamanan data digital.	Murid membuat **profil digital profesional** sebagai simulasi identitas daring seorang pengembang perangkat lunak. Mereka meninjau akun media sosial, portofolio GitHub, dan profil LinkedIn untuk memahami bagaimana jejak digital terbentuk. Selanjutnya, murid mempraktikkan langkah-langkah manajemen identitas daring, seperti mengatur privasi akun, memilih konten yang membangun citra positif, serta menulis deskripsi diri profesional yang mencerminkan etika dan keahlian di bidang RPL. Kegiatan diakhiri dengan refleksi kelompok tentang perbedaan antara citra pribadi dan profesional di ruang siber serta dampaknya terhadap karier di industri teknologi.

Lampiran 3 Desain Asesmen Pendidikan Keamanan Siber

Contoh Desain Asesmen

Contoh desain asesmen formatif:

Tujuan Pembelajaran (contoh)

- **Membedakan** antara perilaku yang baik dan tidak baik saat melakukan panggilan video

Kriteria ketercapaian tujuan pembelajaran (contoh):

a. Murid menunjukkan ekspresi wajah yang ramah (tersenyum, antusias) saat menyapa atau disapa.
b. Murid menggunakan volume suara yang wajar dan terkontrol (tidak berteriak saat bersemangat).
c. Murid menggunakan gestur yang sopan seperti melambaikan tangan untuk menyapa atau berpisah.
d. Murid melihat ke arah layar saat teman atau pendidik sedang berbicara, menunjukkan sikap mendengarkan.
e. Murid menunjukkan usaha untuk tidak memotong pembicaraan orang lain secara sengaja dan mencoba menunggu giliran.
f. Murid tidak menunjukkan ekspresi wajah mengejek (menjulurkan lidah, memelotot) atau meniru suara teman untuk tujuan bercanda yang tidak baik.
g. Murid tidak membuat suara-suara aneh atau keras dengan sengaja untuk mengganggu jalannya panggilan video.

Contoh Desain Asesmen

Aspek	Deskripsi
Jenis Asesmen	Observasi Partisipatif dan Penilaian Kinerja (*Performance Assessment*)
Metode	Simulasi Panggilan Video Berpasangan (*Role-Play*). pendidik membagi murid menjadi pasangan (atau kelompok kecil) dan meminta mereka melakukan panggilan video simulasi (menggunakan tablet, laptop, atau bahkan mainan telepon/layar yang difungsikan sebagai alat komunikasi). pendidik bertindak sebagai fasilitator atau pengamat, mencatat perilaku yang diamati.

Aspek	Deskripsi
Fokus	Pengukuran Perilaku Motorik dan Afektif (ekspresi, volume suara, gestur)
Konteks Pembelajaran	Dilakukan setelah murid diajarkan dan berlatih tentang konsep "perilaku baik" dan "perilaku tidak baik" saat berkomunikasi, yang sejalan dengan Elemen 3 (Etika & Perilaku Digital) Peta RAN Keamanan Siber di tingkat PAUD.

Contoh Rubrik Penilaian (Checklist Observasi pendidik)

Rubrik ini menggunakan skala deskriptif tiga tingkat yang fokus pada frekuensi dan kemandirian murid dalam menunjukkan perilaku yang baik.

No.	Kriteria Ketercapaian Tujuan Pembelajaran (KKTP)	Belum Terlihat (BT) / Skor = 1	Mulai Terlihat (MT) / Skor = 2	Konsisten Terlihat (KT) / Skor = 3
Perilaku Sapaan & Ekspresi				
1.	Menunjukkan ekspresi wajah yang ramah (tersenyum, antusias) saat menyapa atau disapa.	Ekspresi wajah datar atau sedih; tidak merespons sapaan dengan senyum.	Menunjukkan senyum atau ekspresi ramah, tetapi harus diingatkan atau didorong oleh pendidik/ teman.	Secara spontan dan konsisten menunjukkan senyum/ekspresi ramah saat berinteraksi.
2.	Menggunakan gestur yang sopan seperti melambaikan tangan untuk menyapa atau berpisah.	Tidak ada gestur yang digunakan.	Menggunakan gestur (misalnya melambai), tetapi masih ragu atau harus diberi contoh.	Menggunakan gestur yang sesuai (melambai/ gestur sopan lain) secara mandiri saat memulai dan mengakhiri panggilan.

No.	Kriteria Ketercapaian Tujuan Pembelajaran (KKTP)	Belum Terlihat (BT) / Skor = 1	Mulai Terlihat (MT) / Skor = 2	Konsisten Terlihat (KT) / Skor = 3
Kontrol Diri & Perhatian				
3.	Menggunakan volume suara yang wajar dan terkontrol (tidak berteriak saat bersemangat).	Berbicara dengan volume yang sangat tinggi atau berteriak secara berulang.	Volume suara kadang keras, tetapi dapat mengontrol diri setelah diberi isyarat ringan/ diingatkan sekali.	Volume suara selalu wajar, tenang, dan terkontrol sepanjang interaksi.
4.	Melihat ke arah layar saat teman atau pendidik sedang berbicara, menunjukkan sikap mendengarkan.	Sering mengalihkan pandangan atau fokus pada hal lain.	Melihat ke layar, tetapi perhatian teralihkan dengan cepat.	Mempertahankan kontak mata dengan layar/pembicara dalam durasi yang wajar (fokus mendengarkan).
5.	Menunjukkan usaha untuk tidak memotong pembicaraan orang lain secara sengaja dan mencoba menunggu giliran.	Sering memotong pembicaraan orang lain karena terlalu bersemangat.	Kadang memotong, tetapi sadar dan mencoba menunggu giliran setelah diinstruksikan.	Menunggu hingga teman selesai berbicara sebelum merespons atau meminta izin berbicara.
Menghindari Perilaku Negatif				
6.	Tidak menunjukkan ekspresi wajah mengejek atau meniru suara teman.	Menunjukkan ekspresi mengejek, melotot, atau membuat suara-suara aneh untuk mengganggu.	Melakukan perilaku negatif (mengganggu) sekali, tetapi segera berhenti total setelah teguran.	Tidak menunjukkan ekspresi wajah mengejek atau membuat suara-suara aneh/keras.

Contoh Interpretasi Hasil Asesmen Formatif

Total Skor	Kategori	Tindak Lanjut pendidik
15 – 18	**Menguasai (Sangat Baik)**	Berikan peran pengayaan (misalnya, menjadi buddy yang memberi contoh perilaku baik, atau memimpin simulasi berikutnya).
10 – 14	**Berkembang (Baik)**	Lanjutkan praktik dalam skenario yang berbeda. Fokuskan umpan balik pada 1-2 indikator yang masih MT (misalnya, "Tingkatkan usahamu untuk menunggu giliran bicara, ya!").
6 – 9	**Perlu Bimbingan Ekstra (Perlu Perhatian)**	Segera lakukan intervensi. Perilaku ini memerlukan perhatian terfokus dan latihan intensif (remedial) yang disesuaikan dengan kebutuhan anak.

Contoh Rencana Tindak Lanjut Berbasis Data Asesmen Formatif

- Tindak lanjut hasil asesmen formatif harus digunakan untuk perbaikan proses belajar-mengajar yang berkelanjutan

---

Contoh Intervensi untuk murid

1. Intervensi Individual, contohnya:
   - Jika skor rendah pada Indikator Kontrol Suara (No. 3): pendidik melakukan latihan menggunakan alat bantu visual (misalnya, kartu “Suara Kucing” (pelan) dan “Suara Singa” (keras)) untuk mempraktikkan modulasi suara secara sadar.
   - Jika skor rendah pada Indikator Menunggu Giliran (No. 5): pendidik menggunakan “tongkat bicara” atau “kartu antrian” saat simulasi, di mana murid harus memegang benda tersebut sebelum berbicara.
2. Intervensi Kelompok (Latihan Berulang): pendidik mengulang simulasi panggilan video dengan pasangan yang berbeda keesokan harinya, fokus pada indikator yang paling banyak mendapatkan nilai MT.
3. Pengayaan: murid dengan capaian KT ditugaskan untuk mendemonstrasikan etika panggilan video kepada teman-temannya.

Contoh Refleksi dan Perbaikan Pengajaran:

- Jika mayoritas murid mendapat skor rendah pada Indikator No. 4 (Sikap Mendengarkan): Ini mengindikasikan bahwa metode pengajaran pendidik tentang fokus dan perhatian mungkin kurang efektif. pendidik perlu merefleksikan dan merevisi kegiatan berikutnya dengan menambahkan lebih banyak aktivitas yang melibatkan kontak mata dan fokus, seperti kegiatan mirroring (menirukan ekspresi) atau permainan fokus visual.
- Jika hasil menunjukkan sebagian besar murid tidak mampu memberi label "baik" atau "tidak baik" (KKTP 1, yang diukur dengan kuis awal): pendidik harus segera mengulang materi tentang perbedaan perilaku, menggunakan contoh video pendek atau kartu ilustrasi yang lebih jelas.

Contoh desain asesmen Sumatif

Tujuan Pembelajaran

- **Murid mampu membedakan fakta, opini, dan propaganda serta menganalisis dampak negatif penyebaran hoaks.**

Bentuk Asesmen: Analisis Studi Kasus Berbasis Bukti (*Performance Assessment*)

Aspek	Deskripsi	Kebutuhan Asesmen
Bentuk Asesmen	Analisis Komprehensif Studi Kasus Media Campuran.	**Materi Studi Kasus Otentik:** pendidik menyediakan 2 hingga 3 contoh kasus (dalam bentuk teks singkat, tangkapan layar media sosial, atau *headline* berita) yang mengandung campuran: (1) **Fakta**, (2) **Opini**, dan (3) **Propaganda**. Studi kasus ini harus relevan dengan konteks keamanan siber (misalnya, berita palsu tentang kebocoran data atau penipuan keuangan).
Tugas murid	Murid harus: Memberi label (Fakta, Opini, atau Propaganda) pada setiap pernyataan yang diekstraksi dari studi kasus.	

Aspek	Deskripsi	Kebutuhan Asesmen
	▪ Menuliskan justifikasi singkat untuk setiap label, menjelaskan ciri-ciri kebahasaan atau bukti yang mendukung klasifikasinya. ▪ Menganalisis potensi dampak negatif dari bagian yang diklasifikasikan sebagai Propaganda terhadap individu/masyarakat.	Alokasi Waktu: Cukup untuk menganalisis dan menulis justifikasi secara mendalam (misalnya, 60–90 menit).

Kriteria Ketercapaian Tujuan Pembelajaran (KKTP)

Murid dianggap mencapai tujuan pembelajaran jika memenuhi kriteria berikut:

1. Murid mampu mengklasifikasikan minimal 80% pernyataan yang disediakan dengan benar ke dalam kategori Fakta, Opini, atau Propaganda.
2. Murid mampu mengidentifikasi dan menjelaskan ciri-ciri kebahasaan (misalnya, penggunaan kata sifat untuk Opini; referensi sumber terverifikasi untuk Fakta; atau adanya klaim sensasional untuk Propaganda) yang terdapat dalam teks.
3. Justifikasi yang diberikan untuk setiap klasifikasi jelas, ringkas, dan merujuk pada bukti yang relevan.
4. Murid mampu menganalisis potensi kerugian atau dampak sosial yang ditimbulkan jika informasi yang diklasifikasikan sebagai Propaganda dengan mudah dipercayai dan disebarkan.

Rubrik Penilaian

Dimensi Penilaian	Skor 1 (Perlu Bimbingan)	Skor 2 (Cukup)	Skor 3 (Baik)	Skor 4 (Mahir)
Klasifikasi (Akurasi Label)	Akurasi klasifikasi < 50% dari total pernyataan.	Akurasi klasifikasi 50% hingga 69% dari total pernyataan.	Akurasi klasifikasi 70% hingga 89% dari total pernyataan.	Akurasi klasifikasi 90% hingga 100% dari total pernyataan.

Dimensi Penilaian	Skor 1 (Perlu Bimbingan)	Skor 2 (Cukup)	Skor 3 (Baik)	Skor 4 (Mahir)
Justifikasi & Ciri-ciri Bahasa	Gagal memberikan justifikasi atau justifikasi tidak relevan/tidak logis.	Justifikasi ada, tetapi seringkali bersifat umum/tidak spesifik pada target yang sedang diidentifikasi	Justifikasi jelas dan relevan, mulai merujuk pada ciri-ciri kebahasaan (subjektif/ objektif), namun belum konsisten.	Justifikasi sangat jelas dan konsisten, merujuk pada bukti dan secara eksplisit mengidentifikasi ciri-ciri kebahasaan pembeda (misalnya, "ini opini karena menggunakan kata sifat nilai," atau "ini fakta karena sumber dari artikel ilmiah/jurnal penelitian").
Analisis Dampak Hoaks	Tidak mampu mengidentifikasi dampak atau hanya menyebut dampak yang sangat umum (misalnya, "jadi sedih").	Mampu menyebutkan satu atau dua dampak spesifik (misalnya, kerugian waktu), tetapi belum mengaitkan dengan konteks keamanan siber.	Mampu menganalisis potensi dampak sosial dan/atau reputasi yang ditimbulkan, seperti kepanikan atau kerusakan citra diri/kelompok.	Mampu menganalisis dampak yang kompleks (misalnya, konsekuensi hukum, dampak psikologis, atau gangguan infrastruktur/ kepercayaan publik) dari penyebaran propaganda.

Rencana Tindak Lanjut Hasil Asesmen

Hasil asesmen sumatif ini berfungsi sebagai alat ukur capaian akhir dan juga sebagai umpan balik strategis untuk perbaikan program di masa depan

Kategori Capaian	Contoh Tindak Lanjut Murid (Remedial/Pengayaan)	Contoh Tindak Lanjut pendidik (Refleksi dan Perbaikan Program)
Skor Rendah (Skor Total < 6)	Remedial Fokus: Murid diwajibkan mengulang latihan identifikasi ciri-ciri kebahasaan antara fakta dan opini. pendidik dapat	Jika mayoritas murid mendapat skor rendah di Dimensi B (Justifikasi), pendidik perlu merevisi rencana pembelajaran

Kategori Capaian	Contoh Tindak Lanjut Murid (Remedial/Pengayaan)	Contoh Tindak Lanjut pendidik (Refleksi dan Perbaikan Program)
	menggunakan kartu bergambar atau permainan interaktif untuk memvisualisasikan perbedaan kedua konsep tersebut.	unit berikutnya dengan fokus pada latihan *critical reading* dan *source comparison* yang lebih intensif, daripada sekadar memberikan definisi.
Skor Sedang (Skor Total 7 – 9)	Latihan Berkelanjutan: Murid diberikan studi kasus baru yang berfokus pada jenis teks yang paling sulit mereka klasifikasikan (misalnya, Propaganda). Mereka didorong untuk melakukan self-assessment terhadap jawaban mereka sebelumnya	Jika hasil mengindikasikan bahwa kemampuan analisis dampak (Dimensi C) lemah, pendidik harus mengintegrasikan Elemen Kesadaran Hukum (Elemen 5) dan Etika (Elemen 3) secara lebih eksplisit pada unit selanjutnya.
Skor Tinggi (Skor Total ≥ 10)	Pengayaan: Murid ditugaskan untuk: a) Merancang 5 contoh pernyataan yang sengaja dibuat ambigu (sulit dibedakan antara Fakta dan Opini) untuk menguji teman sebaya. b) Membuat panduan verifikasi informasi sederhana (misalnya, infografis atau *flowchart*) untuk diseminasi di kelas/sekolah.	Mempertahankan dan mengembangkan pembelajaran yang sudah baik

Hal-hal Penting Dalam Asesmen

1. Transparansi Rubrik: Rubrik ini harus disosialisasikan kepada murid pada awal unit pembelajaran untuk memastikan mereka mengetahui secara pasti kriteria keberhasilan dan apa yang diukur dalam asesmen ini (transparansi dan objektivitas).
2. Pelaporan: Hasil akhir harus dilaporkan bukan hanya sebagai nilai angka, tetapi juga sebagai narasi deskriptif mengenai kemahiran murid dalam membedakan informasi, yang kemudian digunakan sebagai masukan bagi wali/orang tua.
3. Konversi skor ke dalam rentang tertentu (misal: 0-100) atau ke nilai huruf dapat dilakukan sesuai kebutuhan.

Lampiran 4 Inspirasi Perencanaan Pembelajaran

Inspirasi Perencanaan Pembelajaran Kontekstualisasi Keamanan Siber dengan Pendekatan Pembelajaran Mendalam

PAUD TK B: Aman Bermain Handphone

https://kurikulum.kemendikdasmen.go.id/file/ppkamsiberpaud.pdf

SD Kelas V Bahasa Indonesia: Langkah Aman Berselancar di Dunia Digital

https://kurikulum.kemendikdasmen.go.id/file/ppkamsibersd.pdf

SMP Kelas VII Informatika: Membuat Kata Sandi yang Kuat untuk Melindungi Akun

https://kurikulum.kemendikdasmen.go.id/file/ppkamsibersmp.pdf

SMA Kelas X Informatika: Privasi & Keamanan Akun Digital

https://kurikulum.kemendikdasmen.go.id/file/ppkamsibersma.pdf

SMK Kelas X Informatika: Menerapkan Strategi Perilaku dan Teknis untuk Melindungi Privasi dan Menjaga Keamanan Daring

https://kurikulum.kemendikdasmen.go.id/file/ppkamsibersmk.pdf

Lampiran 5 Perencanaan Pembelajaran Kokurikuler

Kampanye "Mabar Aman": Komunikasi Asik Tanpa Toxic

A. Identitas Umum

Satuan Pendidikan	:	SMP [Nama Sekolah]
Kelas / Fase	:	VIII / D
Tema	:	Etika Berinteraksi dalam Gim Daring
Bentuk Kokurikuler	:	Cara lainnya
Alokasi Waktu	:	100 JP (Sistem Blok)
Lokasi Kegiatan	:	Ruang Kelas, Aula, Laboratorium Komputer, *Learning Management System/LMS*

B. Deskripsi Umum

Aktivitas permainan daring (online gaming) telah bertransformasi menjadi fenomena budaya populer di kalangan remaja, namun sering kali diwarnai oleh pola komunikasi yang negatif (*toxic*), insiden perundungan siber (*cyberbullying*), dan pengabaian terhadap privasi data. Program kokurikuler "Mabar Aman" ini dirancang khusus untuk merespons tantangan tersebut melalui pendekatan **Pembelajaran Mendalam**.

Dalam alokasi durasi 100 Jam Pelajaran (JP), murid tidak hanya diwajibkan untuk memproduksi poster atau video, melainkan diajak untuk melakukan penelusuran mendalam terhadap akar permasalahan melalui riset literasi digital. Mereka akan berdialog dengan pihak yang kompeten (praktisi permainan daring/psikolog), mengasah kompetensi teknis (***hard skill***) melalui serangkaian lokakarya pembuatan konten, hingga melaksanakan siklus revisi karya berdasarkan umpan balik yang konstruktif.

Tujuan utama dari program ini adalah menginternalisasi pada murid kompetensi **Komunikasi** pada tahap **Cakap**, yakni kemampuan untuk menyampaikan pesan kampanye keamanan siber secara akurat, fasih, dan efektif kepada target audiens sebaya mereka.

C. Dimensi Profil Lulusan

1. Dimensi Komunikasi

   - **Subdimensi: Berbicara**

     Target (Cakap - Fase D): Menyampaikan, menggali, dan menanggapi secara lisan berbagai jenis informasi dengan cara yang **cukup tepat, lancar, dan efektif.**

   - **Subdimensi: Menulis**

     Target (Cakap - Fase D): Menyampaikan, menggali, dan menanggapi informasi secara tertulis dengan beberapa jenis teks terpilih dengan cara yang **cukup tepat, lancar, dan efektif.**

2. Dimensi Kewargaan

   - **Subdimensi: Kewargaan Global**

     Target (Cakap - Fase D): Berperilaku sesuai aturan, norma, dan nilai sosial budaya yang berlaku di lingkup global/digital dan menghargai keberagamannya.

D. Praktik Pedagogi

Model pembelajaran inkuiri kolaboratif dengan metode gamifikasi, diskusi, jigsaw, tanya jawab, dan eksibisi

E. Kemitraan Pembelajaran

1. **OSIS/Ekskul Komputer:** Sebagai panitia pelaksana Festival Mabar Aman.
2. **Komunitas E-Sports Lokal / Kampus:** Sebagai narasumber ahli (Kegiatan 3).
3. **Pendidik BK:** Pendampingan materi/psikologis terkait *cyberbullying*.
4. **Pendidik Bahasa Indonesia**: Pemberian materi tentang diksi persuasif dan laras bahasa remaja
5. **Pendidik Informatika dan Seni Budaya**: Pemberian materi tentang desain artistik pada konten digital

F. Pemanfaatan Digital

- **Platform Riset:** Google Scholar, Portal Berita Teknologi.
- **Platform Produksi:** Canva/Adobe Ilustrator/CorelDraw dan sebagainya (Desain), CapCut/YouCut/Filmora dan lainnya (Video editor), Audacity/Adobe Audition dan lain-lain (Audio editing).

- **Platform Diseminasi:** Instagram Reels, TikTok, YouTube Shorts, Website Sekolah, atau platform diseminasi lainnya.

G. Alur Kegiatan Pembelajaran (100 JP)

Tahap 1 **MEMAHAMI (Berkesadaran dan Bermakna)**

Total Waktu: 20 JP

Kegiatan	Rincian Aktivitas
Kegiatan 1: Audit Budaya Digital & Observasi *(4 JP)*	1. **Ice Breaking "Mabar Bingo" (Lembar Kerja 1):** Murid bermain bingo berisi istilah-istilah gim untuk membangun suasana. 2. **Survey "Toxic Meter" (Lembar Kerja 2):** Murid menyebar angket singkat ke warga sekolah (google form/kertas) tentang pengalaman menerima *chat* negatif saat mabar. 3. **Analisis Data Awal:** Murid mengolah data survey sederhana (misal: "Berapa persen murid yang pernah dimaki saat main gim?") dan mempresentasikannya di kelas.
Kegiatan 2: Literasi Jigsaw - Anatomi Keamanan Siber *(8 JP)*	1. **Kelompok Ahli:** Kelas dibagi menjadi 4 kelompok topik: (a) *Cyberbullying*, (b) *Doxing* & Privasi Data, (c) *Account Phishing* & Keamanan Akun, (d) Dampak Psikologis *Toxic Gaming*. 2. **Diskusi Ahli:** Murid membedah artikel/video yang telah dikurasi oleh pendidik terkait topik masing-masing. 3. **Sharing Kelompok Asal:** Murid kembali ke kelompok asal dan saling berbagi tentang temuan mereka.
Kegiatan 3: Bincang Pakar (Talkshow) *(8 JP)*	1. **Sesi Narasumber:** Mengundang praktisi *e-sports*, psikolog remaja, atau ahli keamanan siber (bisa daring/luring). 2. **Eksplorasi Masalah:** Murid melakukan tanya jawab tentang bagaimana para profesional menjaga komunikasi tetap positif meski dalam tekanan. 3. **Refleksi Sesi:** Murid menulis ringkasan "Pelajaran Penting (*Key Takeaways*)" dari narasumber sebagai bahan dasar kampanye.

Tahap 2 **MENGAPLIKASI (Bermakna dan Menggembirakan)**

Total Waktu: 60 JP

Kegiatan	Rincian Aktivitas
Kegiatan 4: Perancangan Strategi Kampanye *(10 JP)*	1. **Penetapan Audiens:** Murid menentukan target kampanye (misal: "Pemain Pemula", "Pemain Kompetitif", atau "Orang Tua"). 2. **Brainstorming Ide (Lembar Kerja 3):** Menggunakan teknik *Design Thinking* (*Empathize & Define*) untuk melakukan brainstorming ide kampanye (gunakan panduan pada LK 3). Poin inti dalam diskusi, misalnya, "Apa masalah utama target audiens?" "Solusi apa yang ditawarkan?" 3. **Pemilihan Media:** Murid menentukan format konten (Video Pendek 60 detik / Poster Infografis / *Podcast / lain-lain*).
Kegiatan 5: Lokakarya Penulisan Naskah (*Copywriting*) *(10 JP)*	1. **Materi Komunikasi Efektif:** Pendidik Bahasa Indonesia memberikan materi tentang diksi persuasif dan laras bahasa remaja. 2. **Drafting:** Kelompok menyusun naskah (*script*) atau *caption*. Fokus pada aspek **Komunikasi Tertulis** yang tepat dan efektif. 3. **Uji Keterbacaan (Lembar Kerja 4):** Tukar naskah antar kelompok. Teman memberikan masukan sesuai rubrik pada LK 4.
Kegiatan 6: Lokakarya Teknis Produksi *(10 JP)*	Pendidik Informatika/Seni Budaya memberikan pelatihan teknis: ▪ *Visual:* Prinsip desain (warna, tipografi), misalnya menggunakan Canva, Adobe, atau perangkat desain digital lainnya. ▪ *Video:* Teknik pengambilan gambar (*angle*, lighting) dan editing dasar (misalnya menggunakan CapCut, YouCut, dan sebagainya). Murid mencoba fitur-fitur aplikasi yang akan digunakan dan membuat mockup atau draft kasar dari konten.
Kegiatan 7: Produksi Konten (Shooting/ Designing) *(20 JP)*	1. **Eksekusi:** Murid melaksanakan pengambilan gambar atau pembuatan desain grafis secara mandiri di lingkungan sekolah. 2. **Pendampingan:** Pendidik bertindak sebagai fasilitator, memastikan murid bekerja sesuai *timeline* dan naskah. 3. **Editing:** Proses penyuntingan dan penyatuan elemen visual/audio.

Kegiatan 8: Uji Coba & Revisi (Feedback Loop) *(10 JP)*	1. **Alpha Test:** Karya "setengah jadi" ditayangkan di depan kelas. 2. **Sesi Kritik Membangun:** Murid lain dan pendidik memberikan masukan tertulis pada *sticky notes* terkait kejelasan pesan dan kualitas visual. 3. **Revisi:** Kelompok memperbaiki karya berdasarkan masukan untuk mencapai kualitas "Cakap" hingga "Mahir".

Tahap 3 **MEREFLEKSI (Bermakna)**

Total Waktu: 20 JP

Kegiatan	Rincian Aktivitas
Kegiatan 9: Festival "Mabar Aman" (Gelar Karya) *(10 JP)*	1. **Persiapan Pameran:** Murid menata stan atau *mini-cinema* di aula/kelas. 2. **Presentasi:** Murid menjelaskan karyanya kepada pengunjung (adik kelas/pendidik lain). Fokus pada kemampuan **Komunikasi Lisan** (menjelaskan ide dengan lancar dan menanggapi pertanyaan). 3. Pengunjung memberikan apresiasi untuk karya terfavorit dan ter-edukatif.
Kegiatan 10: Analisis Dampak & Evaluasi *(5 JP)*	1. **Bedah Respon:** Murid menganalisis komentar atau respon yang diterima saat pameran/di media sosial. 2. **Evaluasi Tim:** Murid melakukan diskusi kelompok tentang dinamika kerja sama dan efektivitas pembagian tugas.
Kegiatan 11: Refleksi Diri & Komitmen *(5 JP)*	1. **Jurnal Refleksi:** Murid melakukan refleksi secara mandiri dengan mengisi jurnal refleksi. 2. Seluruh murid menyusun dan menandatangani "Piagam Mabar Aman" (format terlampir) sebagai tindak lanjut nyata penerapan Kewargaan Global.

H. Asesmen Pembelajaran

Asesmen Formatif

Asesmen ini berbentuk observasi, dan dilakukan pada saat proses pembelajaran, terutama pada kegiatan 5 (lokakarya).

Contoh Rubrik Asesmen

Tujuan Pembelajaran (TP)	Dimensi & Sub Dimensi	Aspek Penilaian (Proses)	Berkembang (Skor 1)	Cakap (skor 2)	Mahir (Skor 3)
TP 1: Murid mampu mengidentifikasi dan mengkritisi pola komunikasi negatif (*toxic*) dalam gim daring.	Dimensi: Kewargaan Sub Dimensi: Kewargaan Global	Identifikasi Masalah & Empati	Analisis masalah masih di permukaan; hanya melarang perilaku *toxic* tanpa menjelaskan alasannya atau dampaknya bagi orang lain.	Mampu menjelaskan hubungan sebab-akibat yang logis (misal: "Ucapan *toxic* membuat mental turun") berdasarkan temuan survei/ riset.	Menunjukkan pemahaman mendalam tentang insight (wawasan baru) psikologi pemain atau dampak jangka panjang yang jarang disadari.

Tujuan Pembelajaran (TP)	Dimensi & Sub Dimensi	Aspek Penilaian (Proses)	Berkembang (Skor 1)	Cakap (skor 2)	Mahir (Skor 3)
TP 2: Murid mampu merancang pesan kampanye "Mabar Aman" yang persuasif (bahasa tepat dan efektif).	Dimensi: Komunikasi Sub Dimensi: Menulis	Perancangan Struktur Pesan (Drafting)	Naskah/Draft pesan melompat-lompat; belum memiliki pembuka (Hook) yang jelas atau solusi masih abstrak.	Struktur pesan lengkap dan runut: (1) Pembuka Menarik (Hook) → (2) Inti Masalah → (3) Solusi Konkret.	Struktur pesan sangat kreatif dan tidak terduga; menggunakan teknik bercerita (*storytelling*) emosional atau humor cerdas.
		Kesesuaian Gaya Bahasa (Diksi)	Bahasa terlalu kaku (seperti buku teks) ATAU bahasa terlalu kasar; istilah gim digunakan dalam konteks yang salah.	Bahasa luwes, santai (kasual), dan sopan; penggunaan istilah gim (noob, carry, ggwp) tepat sesuai konteks audiens remaja.	Bahasa memiliki ciri khas (*voice*) yang kuat; menggunakan permainan kata (*wordplay*) atau rima yang mudah diingat.

Tujuan Pembelajaran (TP)	Dimensi & Sub Dimensi	Aspek Penilaian (Proses)	Berkembang (Skor 1)	Cakap (skor 2)	Mahir (Skor 3)
TP 3: Murid mampu mendiseminasikan gagasan dan berinteraksi digital sesuai norma kesopanan.	Dimensi: Komunikasi Sub Dimensi: Berbicara	Respon terhadap Umpan Balik (*Feedback*)	Menunjukkan sikap defensif (menolak/ marah) atau bingung saat menerima masukan teman/guru pada sesi uji coba.	Menerima masukan/kritik teman dengan sikap terbuka dan apresiatif (santun); mencatat poin perbaikan.	Mampu berdiskusi secara kritis mengenai masukan yang diterima; mengubah kritik tajam menjadi bahan perbaikan yang konstruktif.
		Kolaborasi & Etika Diskusi	Mendominasi pembicaraan dalam kelompok atau pasif (diam saja) saat diskusi perancangan.	Berpartisipasi aktif menyampaikan ide; mendengarkan pendapat teman satu kelompok dengan saksama tanpa memotong.	Menjadi fasilitator bagi teman kelompok; memastikan semua anggota mendapatkan giliran bicara dan idenya dihargai.

Contoh Rencana Tindak Lanjut Asesmen Formatif

Pola Skor	Interpretasi Kondisi	Contoh Tindak Lanjut Langsung (Guru)
Ada Skor 1 pada TP 1 atau TP 3	Murid belum memahami esensi "Aman" & "Netiket". Meskipun naskahnya bagus, karya berpotensi toxic atau melanggar privasi.	Lakukan sesi refleksi mengenai dampak etika/privasi. Berikan Template Naskah baru yang hanya bisa diisi dengan kalimat positif.
Ada Skor 1 hanya pada TP 2	Murid memahami etika, tetapi kesulitan menuangkan ide ke dalam struktur pesan yang runut. Butuh bantuan teknis/kebahasaan.	Pasangkan murid dengan teman yang berstatus Unggul (Mentor Sebaya). Fokus pada perbaikan Struktur Naskah (memastikan ada Hook, Inti, dan Solusi).
Semua Skor minimal 2	Murid sudah memenuhi standar minimal. Mereka siap melanjutkan ke tahap produksi konten (syuting/ desain).	Berikan tanda tangan/stiker "Lolos" pada Lembar Kerja. Dorong untuk segera memulai produksi konten (syuting/desain) sesuai *timeline*.
Mayoritas Skor 3	Murid sangat menguasai materi.	Jadikan Asisten Fasilitator atau *Peer Reviewer* untuk kelompok yang berstatus Kuning. Tantang untuk menambahkan nilai estetika/ kompleksitas teknis (misal: efek *cinematic*).

Asesmen Sumatif

Asesmen ini berbentuk observasi, dan dilakukan pada saat akhir pembelajaran, pada saat gelar karya.

Contoh Rubrik Asesmen

Tujuan Pembelajaran (TP)	Dimensi & Sub Dimensi	Aspek Penilaian	Berkembang (Skor 1)	Cakap (Skor 2)	Mahir (Skor 3)
TP 1: Murid mampu mengidentifikasi dan mengkritisi pola komunikasi negatif (*toxic*) dalam gim daring.	Dimensi: Kewargaan Sub Dimensi: Kewargaan Global	Kedalaman Analisis Masalah	Hanya mampu menyebutkan label umum (misal: "*toxic* itu jahat") tanpa penjelasan spesifik jenis atau dampaknya.	Mampu menginventarisir minimal 3 jenis kata/ frasa *toxic* spesifik dan mengelompokkannya berdasarkan dampak (mental/ privasi).	Mampu memberikan wawasan baru (*insight*) tentang psikologi pemain atau dampak jangka panjang yang jarang disadari.
		Logika Sebab-Akibat	Tidak menjelaskan hubungan sebab-akibat (misal: hanya melarang), alasan masih abstrak.	Mampu menjelaskan hubungan logis antara ucapan toxic dengan penurunan performa tim saat bermain bersama (mabar) atau kesehatan mental.	Analisis sangat tajam, menghubungkan perilaku *toxic* dengan budaya gim yang lebih luas atau sistem kompetisi.
		Alternatif Solusi Bahasa	Solusi hanya berupa larangan ("Jangan lakukan!") tanpa memberikan contoh pengganti.	Mampu memberikan alternatif kalimat positif yang spesifik sebagai pengganti dari kalimat *toxic* (misal: ganti "Noob" dengan "Nice Try").	Memberikan strategi komunikasi yang solutif dan sistematis (misal: teknik pernapasan sebelum mengetik, template chat penyemangat).

Tujuan Pembelajaran (TP)	Dimensi & Sub Dimensi	Aspek Penilaian	Berkembang (Skor 1)	Cakap (Skor 2)	Mahir (Skor 3)
TP 2: Murid mampu merancang dan memproduksi pesan kampanye "Mabar Aman" yang persuasif, menggunakan bahasa yang tepat dan efektif.	Dimensi: Komunikasi Sub Dimensi: Menulis	Struktur Pesan (*Storytelling*)	Pesan tidak terstruktur (melompat-lompat), tidak memiliki pembuka (hook) yang jelas.	Menyusun struktur pesan yang lengkap memuat 3 elemen: Pembuka menarik (Hook), Inti Masalah, dan Solusi/Ajakan konkret.	Struktur pesan sangat kreatif/ tidak terduga, menggunakan teknik bercerita (*storytelling*) emosional atau humor cerdas.
		Gaya Bahasa (*Tone*)	Bahasa terlalu kaku (seperti buku teks) ATAU terlalu kasar/tidak sopan.	Menggunakan ragam bahasa informal/sebaya yang luwes namun tetap mematuhi norma kesopanan (Netiket).	Bahasa memiliki ciri khas (*voice*) yang kuat, menggunakan permainan kata (*wordplay*) atau rima yang mudah diingat (*catchy*).
		Kualitas Teknis Audio Visual	Audio bergema/pecah/ tertutup musik latar; Teks/ font sulit terbaca; Durasi tidak sesuai.	Audio jernih (artikulasi jelas); Teks terbaca nyaman; Durasi pas dan editing rapi sesuai standar platform.	Kualitas produksi memiliki nilai estetika tinggi (cinematic/ profesional); Efek visual/suara memperkuat emosi pesan secara kreatif.

Tujuan Pembelajaran (TP)	Dimensi & Sub Dimensi	Aspek Penilaian	Berkembang (Skor 1)	Cakap (Skor 2)	Mahir (Skor 3)
TP 3: Murid mampu mendiseminasikan gagasan keamanan siber dan berinteraksi digital sesuai norma kesopanan (Netiket).	Dimensi: Komunikasi Sub Dimensi: Berbicara	Penyampaian Lisan (Presentasi)	Bicara terbata-bata, suara terlalu pelan, atau bergantung sepenuhnya pada teks catatan.	Bicara dengan lancar, intonasi jelas, menjelaskan ide dengan bahasa sendiri, dan menjaga kontak mata.	Gaya bicara sangat menarik (*engaging*), mampu melakukan improvisasi dengan luwes jika terjadi kendala.
		Respons & Interaksi	Menjawab pertanyaan dengan bingung/tidak relevan; Menunjukkan sikap defensif (marah/menolak) saat dikritik.	Menjawab pertanyaan audiens dengan relevan dan logis; Menerima masukan/kritik dengan sikap terbuka dan apresiatif.	Jawaban menunjukkan pemikiran kritis mendalam; Mampu mengubah pertanyaan/kritik tajam menjadi bahan diskusi yang memperkaya (diplomatis).
		Etika Digital (Privasi & Keamanan)	Mengandung unsur berisiko SARA/Fisik; Ada potensi pelanggaran privasi (wajah/ID orang lain tanpa izin).	Bebas murni dari unsur SARA/perundungan; Menghormati privasi (sensor nama/ID yang tidak relevan); Mencantumkan sumber aset.	Secara proaktif mempromosikan inklusivitas (keberagaman) dan menjadi model teladan penerapan hak cipta dan privasi.
		Diseminasi Digital (Publikasi)	Mengunggah karya tanpa takarir (caption) jelas atau tanpa tagar relevan.	Mengunggah karya dengan takarir pendukung pesan; Menggunakan tagar sesuai tema; Format sesuai platform.	Mengelola interaksi di kolom komentar media sosial secara aktif-positif; Menggunakan strategi Call to Action (ajakan) yang efektif.

Contoh Pedoman Penilaian

Kategori	Syarat Ketercapaian
Berkembang	Ditetapkan jika salah satu kondisi ini terpenuhi: ▪ Terdapat 3 atau lebih kriteria yang masih di level "Berkembang" ATAU ▪ Kriteria Etika Digital masih "Berkembang" (misal: karya mengandung unsur SARA, toxic, atau pelanggaran privasi).
Cakap	Ditetapkan jika: ▪ Minimal 4 dari 6 kriteria sudah mencapai level "Cakap" atau lebih ▪ Kriteria Etika Digital dan Substansi WAJIB minimal "Cakap".
Mahir	Ditetapkan jika: ▪ *Minimal 4 dari 6 kriteria mencapai level "Mahir" . ▪ TIDAK ADA satupun kriteria yang bernilai "Berkembang" . ▪ Kriteria Etika Digital WAJIB "Mahir".

Contoh Rencana Tindak Lanjut

Kategori	Tindak Lanjut Utama	Aksi Spesifik
Berkembang	Intervensi Remedial	▪ Diberi waktu 1 minggu untuk merevisi elemen yang lemah (misal: audio, etika, atau struktur pesan). ▪ Sesi bimbingan khusus dengan guru Bahasa/ Informatika untuk melatih aspek teknis atau verbal.
Cakap	Apresiasi & Penerapan	▪ Karya dipublikasikan di kanal media sosial resmi sekolah atau mading. ▪ Murid dilantik menjadi "Duta Mabar Aman" yang bertugas memantau etika komunikasi.
Mahir	Pengayaan & Kepemimpinan	▪ Murid menjadi mentor bagi adik kelas (kelas VII) pada projek serupa di masa depan. ▪ Karya didaftarkan ke lomba konten kreatif tingkat kabupaten/kota atau dijadikan materi penyuluhan.

Lembar Kerja 1: Mabar Bingo

"Seberapa 'Gamer' Kamu?"

Nama : _____

Kelas : _____

Game Favorit : _____

PANDUAN CARA BERMAIN (Untuk Murid)

Tujuan: Mendapatkan satu baris lurus (Horizontal, Vertikal, atau Diagonal).

1. **Dengarkan Instruksi:** Pendidik/Fasilitator akan menyebutkan satu definisi atau situasi, atau kamu diminta mencari teman yang tahu arti kata tersebut.
2. **Tandai Kotak:**
   - **Versi Mandiri:** Beri tanda silang (X) pada kotak jika kamu **sering mendengar** atau **tahu arti** istilah tersebut.
   - **Versi Interaktif:** Cari teman sekelasmu yang tahu arti kata di dalam kotak, lalu minta dia menandatangani kotak tersebut (Satu teman maksimal tanda tangan di 2 kotak).
3. **Teriak "MABAR!":** Jika kamu sudah berhasil mendapatkan 5 kotak berturut-turut (satu garis lurus), segera angkat tangan dan teriak **"MABAR!"**.
4. **Jujur itu Keren:** Pastikan kamu benar-benar tahu artinya, ya! Nanti akan kita bahas bersama.

PAPAN BINGO

AFK *(Away From Keyboard)*	**GGWP** *(Good Game Well Played)*	**NOOB** *(Pemula/Cupu)*	**PUSH RANK** *(Kejar Peringkat)*	**ULTI** *(Jurus Andalan)*
BUFF *(Peningkatan Kekuatan)*	**NERF** *(Pengurangan Kekuatan)*	**TOXIC** *(Perilaku Buruk)*	**CARRY** *(Gendong Tim)*	**LAG** *(Koneksi Lemot)*
TOP UP *(Isi Saldo)*	**REPORT** *(Lapor Akun)*	**FREE** *(BONUS)*	**KS / NYAMPAH** *(Kill Steal)*	**CHEATER** *(Curang)*
EZ / EASY *(Gampang Banget)*	**TURU** *(Tidur/Kalah)*	**BY ONE** *(Satu Lawan Satu)*	**GACHA** *(Undian)*	**MABAR** *(Main Bareng)*
BEBAN *(Menyusahkan Tim)*	**SMURF** *(Akun Kecil)*	**CAMAT** *(Cadangan Mati)*	**ROAMING** *(Keliling Peta)*	**SURRENDER** *(Menyerah)*

REFLEKSI SINGKAT (Diskusi)

Setelah permainan selesai, jawablah pertanyaan ini:

1. Dari istilah-istilah di atas, mana 3 kata yang **paling sering** kamu dengar saat bermain gim?

   .....

2. Istilah mana yang terdengar **keren/positif** dan bikin semangat?

   .....

3. Istilah mana yang terdengar **kasar/negatif** dan bisa menyakiti hati teman?

   .....

PANDUAN UNTUK GURU/FASILITATOR

Cara Memimpin Permainan:

Anda tidak perlu menjadi ahli gim untuk memimpin ini. Gunakan Kamus Mini di bawah ini untuk memandu jalannya Bingo atau untuk memverifikasi jawaban murid.

Kamus Mini Istilah Gim:

- **AFK:** Pemain diam saja/meninggalkan permainan.
- **GGWP:** Pujian setelah permainan selesai (permainan bagus).
- **Noob:** Ejekan untuk pemain baru/kurang jago.
- **Toxic:** Berkata kasar, memaki, atau merusak suasana permainan.
- **Buff/Nerf:** Perubahan kekuatan karakter oleh pembuat gim (Buff=makin kuat, Nerf=makin lemah).
- **KS (Nyampah):** Mengambil *kill* yang harusnya milik teman.
- **Turu:** Bahasa Jawa "Tidur", istilah ejekan saat lawan kalah telak (disuruh tidur saja).
- **Ez/Easy:** Ejekan meremehkan lawan ("Gampang banget lawannya").
- **Smurf:** Pemain jago yang menyamar pakai akun baru (level rendah) untuk melawan pemula.

Transisi ke Materi Inti:

Gunakan pertanyaan refleksi nomor 3. Ambil contoh kata "Noob", "Beban", "Ez", atau "Toxic".

- *Tanyakan:* "Bagaimana rasanya kalau kalian dibilang 'Beban'?"
- *Sambungkan:* "Inilah yang akan kita bahas di projek Mabar Aman. Bagaimana kita bisa main seru (GGWP) tanpa harus menyakiti orang lain (Toxic)."

Lembar Kerja 2: Survey “Toxic Meter”

Mendeteksi Tingkat “Racun” dalam Komunikasi Gim Daring

Nama Kelompok : _____

Anggota : _____

Kelas : _____

Tanggal : _____

TUJUAN KEGIATAN

1. Mengumpulkan data nyata tentang pengalaman warga sekolah terkait komunikasi negatif (*toxic*) saat bermain gim daring.
2. Mengidentifikasi jenis ucapan/perilaku *toxic* yang paling sering muncul.
3. Menyajikan data sederhana sebagai dasar pembuatan materi kampanye “Mabar Aman”.

BAGIAN A: INSTRUMEN ANGKET (KUESIONER)

Instruksi:

- Salin atau fotokopi angket di bawah ini sejumlah target responden (misal: 10-15 orang per kelompok).
- Jika menggunakan Google Form, salin pertanyaan ini ke dalam formulir digital kalian.

(Potong di sini untuk dibagikan ke responden)

ANGKET “TOXIC METER” SMP [NAMA SEKOLAH]

Halo! Kami sedang melakukan riset untuk projek sekolah tentang keamanan dan kenyamanan saat bermain gim (*Mabar Aman*). Mohon bantu kami dengan mengisi survei singkat ini secara jujur. Nama kamu tidak perlu ditulis (Anonim).

1. **Apakah kamu bermain gim daring (Mobile Legends, FF, PUBG, Roblox, dll)?**
   - □ Ya
   - □ Tidak (Jika tidak, stop di sini. Terima kasih!)

2. **Seberapa sering kamu bermain gim dalam seminggu?**
   - □ Setiap hari
   - □ 3-4 kali seminggu
   - □ Jarang (1-2 kali atau hanya akhir pekan)
3. **Saat bermain, seberapa sering kamu melihat/menerima chat atau suara negatif (memaki, mengejek, berkata kasar)?**
   - □ Sangat Sering (Hampir setiap main)
   - □ Kadang-kadang
   - □ Jarang sekali
   - □ Tidak pernah
4. **Jenis "Toxic" apa yang paling sering kamu temui? (Boleh pilih lebih dari 1)**
   - □ **Hinaan Skill** (Contoh: "Noob", "Beban", "Bot", "Turu")
   - □ **Kata-kata Kotor/Kebun Binatang** (Memaki kasar)
   - □ **Hinaan Fisik/SARA** (Menghina suku, agama, atau fisik)
   - □ **Blaming** (Menyalahkan teman satu tim terus-menerus)
   - □ **Spamming** (Mengirim pesan tidak jelas berulang-ulang)
   - □ **Ancaman/Doxing** (Mengancam atau menyebar data pribadi)
5. **Bagaimana perasaanmu saat menerima pesan toxic tersebut?**
   - □ Marah / Emosi
   - □ Sedih / Kecewa
   - □ Takut / Cemas
   - □ Biasa saja / Tidak peduli
   - □ Jadi malas main lagi
6. **(Jujur ya!) Apakah kamu sendiri pernah terpancing berkata kasar saat bermain?**
   - □ Pernah
   - □ Tidak Pernah

(Terima kasih atas partisipasimu!)

BAGIAN B: PANDUAN PENGAMBILAN DATA (Untuk Murid)

1. **Target Responden:** Wawancarai atau bagikan angket kepada minimal **10 orang** (bisa teman sekelas, kakak kelas, atau adik kelas).
2. **Etika:** Gunakan bahasa yang sopan saat meminta teman mengisi angket. Contoh: *"Halo, boleh minta waktunya 2 menit untuk bantu tugas projek kami?"*
3. **Privasi:** Jangan memaksa teman untuk menuliskan nama mereka jika mereka tidak mau.

BAGIAN C: REKAPITULASI DATA (Diisi oleh Kelompok)

Setelah angket terkumpul, hitunglah jawabannya dan masukkan ke dalam tabel berikut:

Total Responden: _____ orang

Data yang Dianalisis	Jumlah (Orang)	Persentase (Kira-kira)
Pemain yang Pernah Mengalami Toxic (Menjawab Sering/Kadang di No. 3)	.....	..... %
Perasaan Terbanyak (Jawaban terbanyak di No. 5)	.....	-
Pemain yang Mengaku Pernah Toxic (Jawaban "Pernah" di No. 6)	.....	..... %

Ranking Jenis Toxic (Dari Pertanyaan No. 4):

Urutkan dari yang paling banyak dipilih!

1. .....
2. .....
3. .....

BAGIAN D: KESIMPULAN & DISKUSI

Berdasarkan data di atas, diskusikan pertanyaan ini bersama kelompokmu:

1. **Seberapa parah tingkat "Toxic" di sekolah kita?** (Apakah mayoritas murid merasakannya?)

   Jawab: .....

2. **Apa jenis ucapan toxic yang harus kita lawan lewat kampanye nanti?** (Lihat ranking 1 di Bagian C).

   Jawab: .....

3. Ide Pesan Kampanye:

   Jika banyak teman merasa "Marah" saat dimaki, pesan apa yang bisa menenangkan mereka atau mengingatkan pelaku?

   Ide: .....

Tanda Tangan Pendidik Pendamping: _____

Lembar Kerja 3: Misi Penyelamatan “Mabar”

Design Thinking: Dari Masalah Menjadi Solusi

Nama : _____

Anggota : _____

Kelas : _____

PETA MISI

Kita akan menggunakan cara berpikir desainer (***Design Thinking***) untuk menciptakan solusi kampanye yang tepat sasaran. Ikuti langkah 1 sampai 3 di bawah ini!

Tahap 1 **EMPATHIZE (Kenali Targetmu)**

Buka kembali data survei “Toxic Meter” kalian. Bayangkan satu sosok teman yang paling membutuhkan bantuan kalian.

PROFIL TARGET (PERSONA)

Gambarlah atau tuliskan profil target audiens kalian di kotak ini.

Nama Samaran (Avatar):	**Umur/Kelas: .....**
Gim Favorit:	**Level Skill:** (Pemula / Pro / Iseng)
Masalah Terbesar Dia: (Misal: Sering dimaki “Noob”, sering terpancing emosi, tidak tahu cara report)	**Perasaan Dia Saat Ini:** (Marah / Sedih / Putus Asa / Takut Main Lagi) .....

Tahap 2 **DEFINE (Rumuskan Masalah)**

Bantu target kalian dengan merumuskan masalah intinya dalam satu kalimat jelas.

KALIMAT PERNYATAAN MASALAH (PROBLEM STATEMENT)

Isilah titik-titik di bawah ini untuk menemukan fokus kampanye kalian.

"Si ..... (Nama Target/Avatar tadi)

sangat MEMBUTUHKAN ..... (Kebutuhan/Solusi)

KARENA ..... (Alasan/Insight/Penyebab)."

Contoh: "Si Pemain Pemula sangat MEMBUTUHKAN tutorial cara mematikan fitur chat KARENA dia sering kehilangan konsentrasi akibat baca makian lawan."

Tahap 3 **IDEATE (Curah Gagasan Solusi)**

Sekarang, pikirkan solusi untuk menjawab kebutuhan di atas. Jangan takut salah, tulis semua ide gila kalian!

SOLUSI APA YANG BISA KITA TAWARKAN?

A. **Ide Edukasi (Mengajarkan Sesuatu)**
   - *(Contoh: Tutorial Report Akun)*
   - .....
   - .....

B. **Ide Persuasif (Mengajak/Mencegah)**
   - *(Contoh: Ajakan Stop bilang 'Yatim')*
   - .....
   - .....

C. **Ide Emosional (Menyemangati)**
   - *(Contoh: Kata-kata motivasi saat kalah)*
   - .....
   - .....

KEPUTUSAN FINAL: SOLUSI TERPILIH

Diskusi dengan kelompok, pilih SATU ide terbaik dari Tahap 3 yang paling mungkin kalian buat dan paling berdampak.

1. **Ide Terpilih:** .....
2. **Format Konten:** (Pilih satu)
   - □ Video Pendek (Reels/TikTok/Shorts)
   - □ Poster Digital / Infografis
   - □ Podcast Audio
3. **Judul/Slogan Kampanye:** .....

Ceklis Kelayakan (Diisi Pendidik):

□ Ide relevan dengan masalah (Define)

□ Bahasa sesuai target (Empathize)

□ Pesan positif (Tidak mengandung SARA/Toxic)

Paraf Pendidik: _____

Lembar Kerja 4 - Uji Keterbacaan: “Cek Ombak”

Review Naskah Kampanye Mabar Aman

Kelompok Reviewer (Penilai) : _____

Kelompok Kreator (Pembuat) : _____

Jenis Karya : □ Video

□ Poster

MISI REVIEWER

*Kalian adalah “**Beta Tester**”. Tugas kalian adalah membaca naskah/melihat desain teman kalian dan memastikan konten tersebut **tidak kaku**, **mudah dimengerti**, dan **anti-toxic**.*

Bagian 1 **CEK BAHASA (Flow & Style)**

Bacalah naskah/teks mereka dengan suara lantang. Rasakan alirannya.

1. **Apakah bahasa yang digunakan terasa kaku (seperti buku paket) atau luwes (bahasa gaul/akrab)?**
   - □ **Terlalu Baku/Kaku** (Kurang asik buat remaja)
   - □ **Pas Banget!** (Santai tapi sopan, enak dibaca)
   - □ **Terlalu Kasar/Berlebihan** (Agak mengganggu)
2. **Apakah ada istilah gim yang salah penempatan atau membingungkan?**
   - □ Ada (Tuliskan di bawah)
   - □ Tidak ada, semua istilah tepat.
   - □ *Catatan:* .....

Bagian 2 **CEK PESAN (Clarity)**

Apakah kalian paham maksud dari kampanye mereka?

3. Setelah membaca/melihat karya ini, apakah kamu langsung paham pesan utamanya?
   - □ **Langsung Paham** dalam sekali baca.

- □ **Agak Bingung,** harus baca dua kali.
- □ **Gagal Paham,** maksudnya apa ya?

4. **Jika kamu melihat konten ini di media sosial, apa yang akan kamu lakukan?**
   - □ **Skip** (Membosankan/Tidak menarik)
   - □ **Stop & Baca** (Menarik perhatian)
   - □ **Share** (Sangat keren dan bermanfaat)

Bagian 3 **CEK TOXIC (*Safety*)**

5. **Apakah ada kalimat yang berpotensi menyinggung orang lain (SARA/Body Shaming/ Ejekan)?**
   - □ Aman, bersih dari toxic.
   - □ Hati-hati! Ada bagian yang agak menyerempet bahaya (Sebutkan di bawah).
   - □ *Bagian yang harus dicek ulang: .....*

MASUKAN GGWP (*Good Game Well Played*)

Berikan saran perbaikan agar karya temanmu makin mantap.

NERF THIS! (Kurangi/Hapus)	BUFF THIS! (Pertahankan/Tambah)
(Bagian mana yang harus diperbaiki/ dibuang?)	(Bagian mana yang sudah keren banget?)
.....	.....
.....	.....
.....	.....

RATING FINAL

Beri bintang untuk naskah ini!

- ★ Bintang 1 (Perlu banyak perbaikan)
- ★ Bintang 2 (Sudah oke, poles dikit lagi)
- ★ Bintang 3 (Siap Produksi! Keren!)

Paraf Reviewer: _____

Piagam Mabar Aman

Deklarasi Etika Digital SMP [Nama Sekolah]
Kami, Pelajar SMP [Nama Sekolah],

Menyadari sepenuhnya bahwa dunia maya dan lingkungan permainan daring (***game online***) adalah ruang publik global yang harus dijaga kenyamanan, keamanan, dan kehormatannya.

Kami memahami bahwa di balik setiap ***avatar***, ***nickname***, dan karakter gim, terdapat manusia nyata yang memiliki perasaan dan hak untuk dihormati.

Oleh karena itu, dengan penuh kesadaran dan tanggung jawab, kami berikrar untuk menjunjung tinggi **LIMA KODE ETIK MABAR (Panca Mabar)**:

1. KOMUNIKASI TANPA *TOXIC*

   Kami berjanji untuk selalu menggunakan bahasa yang sopan dan positif. Kami menolak segala bentuk makian, hinaan fisik, rasisme (SARA), dan pelecehan verbal di dalam fitur percakapan (chat) maupun suara (voice chat).

2. ANTI PERUNDUNGAN (*ZERO BULLYING*)

   Kami berjanji untuk menjadi pemain yang suportif. Kami tidak akan merendahkan pemain pemula (newbie), tidak melakukan pengucilan, dan tidak memprovokasi kebencian terhadap lawan maupun kawan satu tim.

3. MENJAGA PRIVASI DAN DATA

   Kami berjanji untuk melindungi data pribadi diri sendiri dan orang lain. Kami tidak akan menyebarkan identitas asli, nomor telepon, atau rahasia orang lain (*doxing*) ke ranah publik tanpa izin.

4. BERMAIN JUJUR (FAIR PLAY)

   Kami berjanji untuk menjunjung tinggi sportivitas. Kami menolak penggunaan cheat, joki, pencurian akun (hack), atau segala bentuk kecurangan yang merusak integritas permainan.

5. SEIMBANG DAN BERKESADARAN

   Kami berjanji untuk tetap mengutamakan kewajiban sebagai pelajar. Kami akan membatasi waktu bermain agar tidak mengganggu kesehatan fisik, mental, dan prestasi akademik.

Demikian piagam ini kami buat sebagai komitmen nyata kami untuk menjadi warga digital yang beradab dan bermartabat.

Main Pintar, Bicara Benar, Mabar Aman!

Ditetapkan di: [Nama Kota]

Tanggal: .....

Atas Nama Seluruh Murid,

(Tanda Tangan Ketua OSIS) *(Tanda Tangan Perwakilan Duta Mabar)*

Mengetahui,

(Tanda Tangan Kepala Sekolah) *(Tanda Tangan Pendidik BK/Kemuridan)*

Tips Pelaksanaan Penandatanganan:

1. **Versi Besar (Banner):** Cetak teks di atas pada banner atau karton manila ukuran besar. Biarkan perwakilan kelas atau seluruh murid membubuhkan tanda tangan mereka di area kosong di sekitar teks piagam.
2. **Versi Digital:** Buat petisi daring (menggunakan Google Form atau Twibbon) di mana murid bisa mengklik "Saya Setuju" sebagai bentuk tanda tangan digital.
3. **Penempatan:** Tempelkan Piagam yang sudah ditandatangani di **Laboratorium Komputer** atau **Majalah Dinding Utama** sebagai pengingat visual yang konstan.

Lampiran 6

Ancaman

Jenis Ancaman	Deskripsi	Modus Operandi	Dampak bagi Anak
Risiko Konten (*Content Risks*)			
Konten Kekerasan & Pornografi	Paparan materi audio/visual yang mengandung kekerasan grafis, pornografi anak, muatan seksual eksplisit atau eksploitasi lainnya.	Muncul melalui situs ilegal, tautan media sosial, konten rekomendasi algoritma, pop-up dalam aplikasi/game, serta berbagi file *peer-to-peer*. Anak sering diarahkan oleh "suggested content" atau tautan dari teman sebaya.	Normalisasi kekerasan, trauma emosional, kebingungan mengenai seksualitas, imitasi perilaku berbahaya, menurunnya konsentrasi belajar.
Hoaks, Disinformasi & Malinformasi	Informasi palsu, menyesatkan, atau dipotong konteks yang memengaruhi cara berpikir anak.	Penyebaran melalui video manipulatif, postingan provokatif, akun propaganda, konten editan AI, serta pesan berantai di platform gim/medsos. Anak rentan mempercayai narasi sederhana yang memancing emosi.	Salah persepsi, intoleransi, kesulitan memilah informasi, gangguan proses belajar, potensi radikalisasi.
Konten Kebencian (*Hate Speech*)	Ungkapan kebencian berbasis SARA, diskriminasi, penghinaan kelompok tertentu.	Komentar bermuatan kebencian di medsos, forum daring, *streaming game*, atau video provokatif yang mempromosikan intoleransi.	Menurunnya empati, munculnya perilaku agresif, sikap diskriminatif, terjadinya konflik antar siswa.
Risiko Kontak (*Contact Risks*)			
Online Grooming	Upaya manipulatif pelaku untuk membangun hubungan emosional dengan anak sebelum melakukan eksploitasi seksual.	Pelaku menyamar sebagai orang lain dengan profil yang menarik, memberikan perhatian/pujian, mengajak obrolan privat di game/ medsos, hingga meminta foto pribadi. Setelah korban percaya, pelaku	Eksploitasi seksual, trauma, rasa bersalah atau malu, kerusakan psikologis jangka panjang, prestasi belajar menurun.

Jenis Ancaman	Deskripsi	Modus Operandi	Dampak bagi Anak
		mengarahkan percakapan ke tema sensual.	
***Sextortion* (Pemerasan Seksual)**	Pemerasan menggunakan foto/ video sensitif anak.	Pelaku mengancam menyebarkan konten intim yang sebelumnya diminta, dicuri, atau dimanipulasi (*deepfake*). Pelaku memaksa korban memberikan foto tambahan, uang, atau akses akun.	Trauma berat, kehilangan rasa aman, gangguan tidur, risiko bunuh diri.
Imperson-ation* & *Spoofing	Penyalahgunaan identitas orang yang dipercaya anak.	Pelaku membuat akun palsu menyerupai guru, orang tua, atau teman, mengirim email sekolah palsu, atau meniru gaya bicara via *voice-cloning* untuk meminta data, foto, atau uang.	Penipuan, pencurian data pribadi, hilangnya kepercayaan sosial, risiko eksploitasi lanjutan.
Risiko Perilaku (*Conduct Risks*)			
***Cyberbully-ing*/Perun-dungan Daring**	Perilaku merendahkan atau menyerang anak melalui media digital.	Pelaku mengirim komentar kasar, menyebarkan foto/ video tanpa izin, membuat meme penghinaan, atau mempermalukan korban di grup kelas. Bisa terjadi terus-menerus dan melibatkan banyak pelaku.	Depresi, isolasi sosial, prestasi akademik menurun, stres berat, risiko ide bunuh diri.
Pelibatan Anak sebagai Pelaku	Anak terlibat perilaku ilegal atau merugikan tanpa memahami konsekuensi hukum maupun etika.	Anak menyebar hoaks, doxing, membuat akun palsu, memanfaatkan konten ilegal, atau membully siswa lain. Terkadang mengikuti tantangan viral berbahaya.	Konsekuensi hukum, stigma sosial, catatan pendidikan negatif, rusaknya reputasi diri/ keluarga.

Jenis Ancaman	Deskripsi	Modus Operandi	Dampak bagi Anak
***Hacking* & Akses Tanpa Izin**	Upaya masuk ke akun, aplikasi, atau sistem tanpa hak akses.	Memanfaatkan kata sandi lemah, mencoba exploit sederhana, menggunakan tools untuk deface, atau menebak OTP/kredensial. Banyak anak melakukannya sebagai "tantangan teknis" tanpa memahami risiko hukum.	Catatan kriminal, hilangnya masa depan pendidikan/ kerja, kerugian bagi korban lain, paparan ke jaringan kejahatan digital.
Risiko Komersial (*Commercial Risks*)			
Phishing* & *Malware	Upaya mencuri data atau merusak perangkat melalui tautan/aplikasi berbahaya.	Tautan hadiah palsu, situs login tiruan, unduhan game/ aplikasi ilegal, atau lampiran email yang mengandung malware. Pelaku meniru platform resmi seperti sekolah, marketplace, atau bank.	Kehilangan akun, identitas dicuri, kerugian finansial keluarga, perangkat rusak.
Penipuan Daring (*Scam*)	Penipuan berbasis hadiah, undian, langganan premium, atau belanja online.	Iklan harga sangat murah, pesan "hadiah menang", tautan promo fiktif, hingga penjual palsu. Anak juga bisa tertipu top-up game bodong.	Kerugian finansial, rasa malu, kehilangan kepercayaan diri dan terhadap teknologi.
Online Love Scam	Relasi palsu berbasis rayuan emosional untuk memanipulasi anak.	Pelaku membangun hubungan romantis palsu, memuji berlebihan, meminta foto pribadi, lalu berujung permintaan uang atau pemerasan.	Trauma emosional, kerugian finansial, kesulitan membangun relasi sehat.
Judi Online & Game Berbayar Ilegal	Taruhan atau transaksi ilegal dalam permainan digital.	Skin betting, mengenalkan konsep koin sebagai bagian dari permainan gim, kasino online via situs/aplikasi tersembunyi, pembelian item ilegal, hingga manipulasi top-up.	Kecanduan, hutang, risiko kriminal, penurunan prestasi belajar.

Jenis Ancaman	Deskripsi	Modus Operandi	Dampak bagi Anak
Pencurian Identitas Digital	Pengambilan data pribadi anak untuk tujuan ilegal.	Pelaku mengakses akun, mengambil NIK/data sekolah, atau membuat identitas palsu untuk transaksi ilegal.	Penyalahgunaan identitas, kerugian finansial, masalah hukum di kemudian hari.
Eksploitasi Ekonomi Anak	Pemanfaatan anak untuk memperoleh keuntungan finansial secara tidak etis atau ilegal.	Anak didorong menjual akun game, dibuat membuat konten eksploitasi, atau bekerja secara daring dengan tekanan berlebihan.	Kehilangan hak belajar, kelelahan, stres, gangguan perkembangan sosial.
Risiko Sistem (*Systemic Risks*)			
AI *Harms* (Deepfake, Manipulasi AI Generatif)	Penggunaan AI untuk membuat konten palsu yang menyerupai anak atau figur yang dikenal.	Deepfake wajah anak, suara palsu via voice cloning, pesan dari "guru palsu", atau chatbot yang mengumpulkan data pribadi untuk tujuan berbahaya.	Kerusakan reputasi, pemerasan, penyebaran informasi palsu, hilangnya kepercayaan pada lingkungan sekolah.
Profiling* & *Datafication	Pengumpulan dan pemetaan perilaku anak oleh platform digital.	Tracking aktivitas, preferensi, durasi penggunaan, pola interaksi, dan segmentasi untuk iklan yang dipersonalisasi.	Eksploitasi data, manipulasi perilaku, terjebak dalam bubble informasi.
***Surveillance* & Bias Algoritmik**	Pemantauan digital atau pengambilan keputusan otomatis yang tidak transparan dan berpotensi bias.	Algoritma rekomendasi yang mendorong konten ekstrem, filter otomatis yang menilai perilaku anak secara tidak proporsional, serta pembatasan akses tanpa penjelasan.	Paparan konten ekstrem, diskriminasi algoritmik, dampak pada kesejahteraan mental dan rasa keadilan.
Risiko pada EdTech	Pengumpulan dan penyimpanan data siswa secara berlebihan melalui aplikasi pembelajaran.	Tracking tugas, rekaman video kelas, pengambilan metadata, penyimpanan riwayat aktivitas, serta pembagian data ke pihak ketiga.	Pelanggaran privasi, kebocoran data siswa, penyalahgunaan komersial, ketidakpercayaan terhadap platform belajar.

Lampiran 7

Contoh Template

Memorandum Of Understanding (Mou) Antara Sekolah Dan Lembaga

Nota Kesepakatan Tentang Kerja Sama Pengembangan Pendidikan Keamanan Siber

NOMOR: *[Nomor Surat Sekolah]*

NOMOR: *[Nomor Surat Lembaga]*

Pada hari ini, [Hari], tanggal [Tanggal] bulan [Bulan] tahun [Tahun] ([DD/MM/YYYY]), di [Lokasi Penandatanganan], kami yang bertanda tangan di bawah ini:

Pihak-Pihak yang Bersepakat

Pihak Pertama (Sekolah)

Nama Institusi : [Nama Sekolah Lengkap]

Alamat : [Alamat Lengkap Sekolah]

Diwakili Oleh : [Nama Kepala Sekolah/Jabatan]

Jabatan : [Kepala Sekolah/Jabatan Resmi]

Selanjutnya disebut sebagai **PIHAK PERTAMA**.

Pihak Kedua (Lembaga)

Nama Lembaga : [Nama Lembaga/Organisasi Lengkap]

Jenis Lembaga : [Contoh: Lembaga Swadaya Masyarakat/Pusat Studi/Balai Diklat]

Alamat : [Alamat Lengkap Lembaga]

Diwakili Oleh : [Nama Direktur/Ketua/Jabatan]

Jabatan : [Direktur Eksekutif/Ketua/Jabatan Resmi]

Selanjutnya disebut sebagai **PIHAK KEDUA**.

PARA PIHAK sepakat untuk mengadakan Nota Kesepahaman yang mengatur kerja sama dengan ketentuan sebagai berikut:

Pasal 1

Maksud dan Tujuan

1. Maksud dari Nota Kesepahaman ini adalah sebagai pedoman bagi **PARA PIHAK** dalam melaksanakan kerja sama pendidikan keamanan siber di lingkungan sekolah.
2. Tujuan dari Nota Kesepahaman ini adalah:
   a. Meningkatkan kesadaran siswa dan guru terhadap risiko dan ancaman di dunia siber.
   b. Menyediakan akses bagi siswa dan guru terhadap materi dan pelatihan keamanan siber yang kredibel.
   c. Mendukung terwujudnya ekosistem sekolah yang aman dan bertanggung jawab secara digital.

Pasal 2

Ruang Lingkup Kerja Sama

Ruang Lingkup Nota Kesepahaman ini meliputi:

1. **Edukasi dan Pelatihan:** Pelaksanaan seminar, *workshop*, dan pelatihan literasi serta keamanan siber untuk siswa, guru, dan tenaga kependidikan.
2. **Penyediaan Materi:** Pengembangan dan/atau penyediaan modul, *toolkit*, atau materi ajar mengenai keamanan siber.
3. **Pengembangan Kebijakan:** Konsultasi dan pendampingan bagi sekolah dalam merumuskan kebijakan internal terkait penggunaan teknologi dan keamanan data.
4. **Program Pendampingan:** Penyelenggaraan kegiatan pendukung lainnya yang berkaitan dengan peningkatan budaya aman berinternet.

Pasal 3

Jangka Waktu

1. Nota Kesepahaman ini berlaku untuk jangka waktu **[Durasi, contoh: 2 (dua) tahun]** terhitung sejak tanggal penandatanganan.
2. Nota Kesepahaman ini dapat diperpanjang atau diakhiri atas kesepakatan tertulis **PARA PIHAK**.

Pasal 4

Hak dan Kewajiban

4.1 Hak dan Kewajiban PIHAK PERTAMA (Sekolah)

- **Hak:** Menerima manfaat program edukasi, materi, dan pendampingan yang diselenggarakan oleh PIHAK KEDUA.
- **Kewajiban:** Memberikan dukungan administratif, menyediakan sarana dan prasarana yang diperlukan, serta mengoordinasikan partisipasi peserta.

4.2 Hak dan Kewajiban PIHAK KEDUA (Lembaga)

- **Hak:** Melakukan sosialisasi program dan mengumpulkan data terkait pelaksanaan program (dengan persetujuan PIHAK PERTAMA).
- **Kewajiban:** Merencanakan, menyiapkan, dan melaksanakan program pendidikan keamanan siber dengan standar yang telah disepakati.

Pasal 5

Pembiayaan

Segala biaya yang timbul sebagai akibat pelaksanaan kegiatan operasional dari Nota Kesepahaman ini akan diatur dan disepakati lebih lanjut dalam Perjanjian Kerja Sama (PKS) atau perjanjian pelaksana teknis, sesuai dengan ketentuan dan sumber pendanaan **PARA PIHAK**.

Pasal 6

Kerahasiaan

PARA PIHAK sepakat untuk menjaga kerahasiaan semua informasi atau data, termasuk data siswa dan operasional, yang bersifat sensitif dan tidak dipublikasikan yang diperoleh selama pelaksanaan kerja sama.

Pasal 7

Penyelesaian Perselisihan

1. Apabila timbul perselisihan dalam pelaksanaan Nota Kesepahaman ini, **PARA PIHAK** sepakat untuk menyelesaikannya secara musyawarah untuk mencapai mufakat.
2. Apabila penyelesaian secara musyawarah tidak tercapai, **PARA PIHAK** sepakat untuk

menempuh jalur hukum sesuai dengan peraturan perundang-undangan yang berlaku di Indonesia.

Pasal 8

Penutup

Nota Kesepahaman ini dibuat dan ditandatangani oleh **PARA PIHAK** di [Lokasi Penandatanganan] pada tanggal tersebut di atas, dalam rangkap 2 (dua) asli, bermaterai cukup, dan masing-masing pihak menerima satu rangkap yang mempunyai kekuatan hukum yang sama.

PIHAK PERTAMA	**PIHAK KEDUA**
(.....)	(.....)

KEMENTERIAN PENDIDIKAN DASAR DAN MENENGAH
BADAN STANDAR, KURIKULUM, DAN ASESMEN PENDIDIKAN